

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

**MINISTRE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE**

**CONFERENCE REGIONALE DES ETABLISSEMENTS
UNIVERSITAIRES DE LA REGION CENTRE**

**OFFRE DE FORMATION DE 3^{ème} CYCLE
EN VUE DE L'OBTENTION DU DOCTORAT
AU TITRE DE L'ANNÉE UNIVERSITAIRE 2024/ 2025**

La qualité de l'Établissement de l'enseignement supérieur :

Etablissement « Point focal » ☐

Etablissement « Partenaire » ☒

Projet de la Formation Doctorale par filière

ETABLISSEMENT	DOMAINE	FILIERE
École supérieure en Sciences et Technologies de l'Informatique et du Numérique (ESTIN)	Mathématiques & Informatique	Informatique

Structures d'adossement du projet de formation doctorale

☒	Code(s) du Laboratoire(s) de Recherche : C44601100, C0792300
☒	Autre (à préciser) : Unité de recherche en sciences des données et applications (CERIST)

Type de l'école doctorale

Type	
☒	Ecole doctorale régionale
☐	Ecole doctorale nationale

Responsable de la formation doctorale

SEBAA Abderrazak

1- Domiciliation de la formation doctorale :

Établissement	Faculté / Institut	Département
École supérieure en Sciences et Technologies de l'Informatique et du Numérique (ESTIN)		

2- Responsable du projet de formation doctorale :

(Professeur, MCA)

Nom & prénom : SEBAA Abderrazak

Grade : Maître de Conférences A

☎: +213550098094

Fax :

E - mail : sebaa@estin.dz

Joindre un CV succinct en annexe de l'offre de formation (selon modèle joint).

3- Bilan des formations doctorales en cours dans la filière

Y a-t-il des formations doctorales en cours ?

☒

OUI

☐

NON

Si oui, veuillez renseigner le tableau suivant :

Année d'habilitation	Nombre total d'inscrits	Nombre de doctorants ayant soutenu	Nombre de doctorants n'ayant pas soutenu
2021-2022	14	00	14
2022-2023	14	00	14

4- Objectifs assignés à la formation doctorale (joindre synthèse selon annexe2)

Voir annexe2.

5- Les capacités effectives : Moyens humaines et matériels déployés (annexe3)

Voir annexe3.

6- Comité de formation doctorale :

Nom et Prénom*	Grade	Filière	Spécialité	Établissement de rattachement	Qualité (Responsable, directeur de thèse, directeur du labo d'adossement, VRPG/DAPG)
SEBAA Abderrazak	MCA	Informatique	Informatique	ESTIN	Responsable
ELMIR Youssef	MCA	Informatique	Informatique	ESTIN	DAPG
DEJNADI Ali	MCB	Electronique	Electronique	ESTIN	Directeur du labo d'adossement
SLIMANI Hachem	Pr.	Informatique	Informatique	Université de Béjaia	Directeur du labo d'adossement
TARI Abdelkamel	Pr	Informatique	Informatique	ESTIN	Directeur de thèse
AZOUAOU Faïçal	Pr	Informatique	Informatique	ESTIN	Directeur de thèse
KHANOUCHE Mohamed Essaid	MCA	Informatique	Informatique	ESTIN	Directeur de thèse
BELAID Ahror	Pr	Informatique	Informatique	CERIST	Directeur de thèse
FARAH Zoubeyr	MCA	Informatique	Informatique	Université de Béjaia	Directeur de thèse
DENNAI Abdeslam	Pr	Informatique	Informatique	Université de Béchar	Directeur de thèse
LAOUID Abdelkader	Pr.	Informatique	Informatique	Université d'El oued	Directeur de thèse

Le nom et le prénom du responsable de la formation est mis en première position, il doit être de la même filière que la formation doctorale.

(*) Joindre CV selon annexe 1.

7- Équipe d'encadrement* des thèses de doctorat (Pr, MCA, DR, MRA) :

Nom et Prénom**	Grade	Filière	Spécialité	Établissement de rattachement	Nombre de thèses en cours d'encadrement	Nombre de thèses à encadrer
TARI Abdelkamel	Pr.	Informatique	Informatique	ESTIN	05	03
AZOUAOU Faïçal	Pr.	Informatique	Informatique	ESTIN	05	04
KHANOUCHE Mohamed Essaid	MCA	Informatique	Informatique	ESTIN	04	01
SEBAA Abderrazak	MCA	Informatique	Informatique	ESTIN	07	07
ELMIR Youssef	MCA	Informatique	Informatique	ESTIN	04	09
FARAH Zoubeyr	MCA	Informatique	Informatique	Université de Béjaia	03	01

BELAID Ahror	Pr.	Informatique	Informatique	CERSIT	03	01
DENNAI Abdeslam	Pr.	Informatique	Informatique	Université de Béchar	03	01
LAOUID Abdelkader	Pr.	Informatique	Informatique	Université d'El oued	04	01

(*) Equipe d'encadrement = Directeurs de thèses mentionnés dans le tableau 6 (CFD).

(**) Joindre CV selon annexe 1.

8- Sujets des thèses proposés :

(Les enseignants ayant dépassé le nombre maximal d'encadrement autorisé ne peuvent pas proposer de nouveaux sujets de thèses –sauf filières stratégiques-) :

N°	Sujet de thèse proposé(*)	Filière du sujet de thèse	Spécialité du sujet de thèse	Directeur de Thèse
1	Exploring transferability of explanations in Machine Learning	Informatique	Intelligence Artificielle	Dr. SEBAA Abderrazak Pr. MEPHU NGUIFO Engelbert
2	Enhancing Chatbot Performance with Large Language Models (LLMs)	Informatique	Intelligence Artificielle	Pr. LAOUID Abdelkader Pr. AZOUAOU Faïçal
3	Développement d'interfaces homme-robot intuitives basées sur des approches neuro-symboliques pour une communication et une collaboration efficaces entre les humains et les cobots dans les environnements médicaux	Informatique	Intelligence Artificielle	Dr. ELMIR Youssef Dr. DJENADI Ali
4	Intégration Multimodale d'Images 2D et de Nuages de Points 3D pour une Classification d'Images Plus Précise : Application à la Classification d'Images d'Herbiers	Informatique	Intelligence Artificielle	Dr. SEBAA Abderrazak Dr. SKLAB Youcef
5	Enhancing Explainability and Interpretability of Deep Learning Models for Security Applications	Informatique	Intelligence Artificielle	Pr. BELAID Ahror
6	Analyzing the Psychological Consequences of Intrusion and Manipulation in Recommender Systems for Fake Recommendations Distribution	Informatique	Intelligence Artificielle	Pr. AZOUAOU Faïçal Dr. BERBAGUE Chemseddine
7	Modèles de Transformers pour le diagnostic des troubles dépressifs à partir des données Électroencéphalogrammes	Informatique	Intelligence Artificielle	Dr. ELMIR Youssef Dr. BOUBCHIR Larbi
8	IA générative pour la conception d'agents de cyberattaques intelligents	Informatique	Réseaux et sécurité	Pr. TARI Abdelkamel Pr. ADI Kamel
9	Approche guidée par la qualité de données pour une gestion automatique des systèmes de systèmes cyber-physiques dynamiques	Informatique	Réseaux et sécurité	Dr. SEBAA Abderrazak Dr. GUERMOUCHE Nawal
10	Privacy-preserving data analytics at scale - Application to Healthcare	Informatique	Intelligence Artificielle	Dr. ELMIR Youssef Pr. KECHADI Mohand-Tahar

11	Real-Time anomaly detection framework for cyberattacks targeting sensor data in Cyber-Physical Systems	Informatique	Réseaux et sécurité	Dr. FARAH Zoubeyr Dr. CHELOUAH Leila
12	Méthodes d'Intelligence Artificielle pour l'Internet du comportement	Informatique	Intelligence Artificielle	Dr. KHANOUCHE Mohamed Essaid
13	Neuro-Symbolic Approaches for Advanced Biological Data Management and Analysis	Informatique	Intelligence Artificielle	Dr. ELMIR Youssef Pr. NOURINE Lhouari
14	Network Intrusion Detection	Informatique	Réseaux et sécurité	Pr. AZOUAOU Faïçal Dr. Hani Ragab Hassen
15	Assurance de vie privée dans les contrats intelligents	Informatique	Réseaux et sécurité	Pr. TARI Abdelkamel Pr. ADI Kamel
16	Analyse Multi-Omique Intégrative pour la Prédiction des Interactions Protéine-Protéine dans la Découverte de Médicaments : Vers des Interventions Thérapeutiques Ciblées	Informatique	Intelligence Artificielle	Dr. SEBAA Abderrazak Dr. DAOUDI Meroua
17	Multi-source Data Integration for Enhanced Flood Prediction	Informatique	Intelligence Artificielle	Dr. ELMIR Youssef Pr. AMIRA Abbes
18	Cybersécurité des données médicales des patients à base des STaaS-Cloud	Informatique	Réseaux et sécurité	Pr. DENNAI Abdeslam Dr. ELMIR Youssef
19	Advancing Radiology Reporting through Collaborative AI-Enabled Approaches	Informatique	Intelligence Artificielle	Pr. AZOUAOU Faïçal Dr. LEKEHALI Somia
20	Security and Privacy in Large-Scale Systems (e.g., LLM, GenAI, Edge, etc)	Informatique	Réseaux et sécurité	Dr. SEBAA Abderrazak Pr. TARI Zahir
21	Amélioration de la détection d'anomalies dans les séquences vidéo pour la sécurité énergétique	Informatique	Intelligence Artificielle	Dr. ELMIR Youssef Dr. BENKABOU Seif Eddine
22	Sécurité dans l'Internet des comportements (IoB)	Informatique	Réseaux et sécurité	Pr. TARI Abdelkamel Dr. DJEBARI Nabil
23	LLMs at the rescue of fake news -- Case study to journalism	Informatique	Intelligence Artificielle	Dr. ELMIR Youssef Pr. KECHADI Mohand-Tahar
24	Reinforcement learning for optimization of vehicle platooning on highways	Informatique	Intelligence Artificielle	Dr. SEBAA Abderrazak Dr. FARHI Nadir
25	Apprentissage multivue pour la détection d'anomalies cardiaques à partir de données multi-sources	Informatique	Intelligence Artificielle	Dr. ELMIR Youssef Dr. BENABDESLEM Khalid
26	Mise en place d'un jumeau numérique pour améliorer l'apprentissage des drones dans le suivi d'objets en vol	Informatique	Intelligence Artificielle	Pr. AZOUAOU Faïçal Pr. BOUNCEUR Ahcene
27	Intelligent models for Privacy and trust in Internet of Things ecosystems	Informatique	Réseaux et sécurité	Dr. SEBAA Abderrazak Dr. ALOUACHE Lylia
28	Adaptive Defense Strategies Using LLMs: Developing Context-Aware Security Protocols for Dynamic Threat Landscapes	Informatique	Réseaux et sécurité	Dr. ELMIR Youssef Dr. Yassine Himeur

(*) Les sujets de thèse doivent répondre aux objectifs et priorités cités dans la note méthodologique. Pour chaque sujet de thèse, prière de renseigner, le plan de recherche correspondant (Voir annexe 4).

9- Parcours de formation ouvrant droit à la participation au concours d'accès :

L'offre de formation de 3^{ème} cycle correspond à une filière impliquant toutes les spécialités de la même filière, avant ou après harmonisation, dispensés à l'échelle nationale.

10- Programme de la formation de renforcement des connaissances :

Activités	Semestre 1	Semestre 2
Cours de renforcement de spécialité en rapport avec la formation Doctorale	Data Science / Sécurité 15 h	Techniques avancées de l'IA/Cryptographie avancée 15 h
Cours de méthodologie de recherche	10 h	10 h
Séminaires	01 séminaire par 15 jours dans le cadre des activités du laboratoire de recherche de l'ESTIN	01 séminaire par mois dans le cadre des activités du laboratoire de recherche de l'ESTIN

Important :

- Les cours dispensés entrent dans le cadre des charges pédagogiques des enseignants chercheurs.
- Le volume horaire des cours de renforcement des connaissances est fixé à deux (02) heures par semaine. Ces cours peuvent être organisés par spécialité ou regroupés par filière.
- Une formation complémentaire est assurée selon la réglementation en vigueur.
- Le carnet de doctorant est obligatoire pour la validation des acquis et pour le suivi du doctorant, qui sera introduit dans la plateforme numérique PROGRES.

11- Intervenants dans la formation de renforcement des connaissances :

Noms et Prénoms	Qualité*	Nature de l'intervention (Cours, atelier, conférence, etc...)
TARI Abdelkamel	Enseignant-chercheur	Conférences et direction de thèses
AZOUAOU Faical	Enseignant-chercheur	Conférences et direction de thèses
KHANOUCHE Mohamed Essaid	Enseignant-chercheur	Conférences et direction de thèses
SEBAA Abderrazak	Enseignant-chercheur	Conférences et direction de thèses
ELMIR Youssef	Enseignant-chercheur	Conférences et direction de thèses
FARAH Zoubeyr	Enseignant-chercheur	Conférences et direction de thèses
BELAID Ahror	Enseignant-chercheur	Conférences et direction de thèses
DENNAI Abdeslam	Enseignant-chercheur	Conférences et direction de thèses

GHAZLI Abdelkader	Enseignant-chercheur	Conférences et direction de thèses
LAOUID Abdelkader	Enseignant-chercheur	Conférences et direction de thèses
ISSAADI Badredine	Enseignant-chercheur	Conférences et codirection de thèses
MEDJOUJ Rafik	Enseignant-chercheur	Conférences et codirection de thèses
KACIMI Farid	Enseignant-chercheur	Conférences et codirection de thèses
BERBAGUE Chemseddine	Enseignant-chercheur	Conférences et codirection de thèses
CHELOUAH Leila	Enseignante-chercheuse	Conférences et codirection de thèses
AIT TALEB Samiha	Enseignante-chercheuse	Conférences et codirection de thèses
DAOUDI Meroua	Enseignante-chercheuse	Conférences et codirection de thèses
LEKEHALI Somia	Enseignante-chercheuse	Conférences et codirection de thèses
EL BOUHISSI Houda	Enseignante-chercheuse	Conférences et direction de thèses
AHMED NACER Mohamed	Professeur associé	Conférences et direction de thèses
BOUFAIDA Mahmoud	Professeur associé	Conférences et codirection de thèses
ADI Kamel	Professeur associé	Conférences et codirection de thèses
KECHADI M. Tahar	Professeur associé	Conférences et codirection de thèses
NAÏT-ABDESSELAM Farid	Professeur associé	Conférences et codirection de thèses
AMIRAT Yacine	Professeur associé	Conférences et codirection de thèses
CHIBANI Abdelghani	Professeur associé	Conférences et codirection de thèses
AIT AMEUR Yamine	Professeur associé	Conférences et codirection de thèses
ALILI Mohamed	Professeur associé	Conférences et codirection de thèses
SAIS Lakhdar	Professeur invité	Conférences et codirection de thèses
KHEDDOUCI Hamamache	Professeur invité	Conférences et codirection de thèses
NOURINE Lhouari	Professeur invité	Conférences et codirection de thèses
TARI Zahir	Professeur invité	Conférences et codirection de thèses
DJOUDI Mahieddine	Professeur invité	Conférences et codirection de thèses

BELLATRECHE Ladjel	Professeur invité	Conférences et codirection de thèses
BOUABDELLAH Abdelmadjid	Professeur invité	Conférences et codirection de thèses
BOUNCEUR Ahcène	Professeur invité	Conférences et codirection de thèses
POTTIER Bernard	Professeur invité	Conférences et codirection de thèses
ZIANE Yasmina	Enseignante-chercheuse	Conférences et codirection de thèses
KHERBACHI Sonia	Enseignante-chercheuse	Conférences et codirection de thèses
BENKHIDER Naima	Enseignante-chercheuse	Conférences et codirection de thèses
KHERBACHI Hamid (Associé)	Professeur associé	Conférences et codirection de thèses
BENABDESLAM Khalid	Enseignant-chercheur	Conférences et codirection de thèses
LARABI Mohamed-Chaker	Enseignant-chercheur	Conférences et codirection de thèses
BENKABOU Seif Eddine	Enseignant-chercheur	Conférences et codirection de thèses
AMIRA Abbes	Professeur invité	Conférences et codirection de thèses
HIMEUR Yassine	Enseignant-chercheur	Conférences et codirection de thèses
ALOUACHE Lylia	Enseignante-chercheuse	Conférences et codirection de thèses
Hani Ragab Hassen	Enseignant-chercheur	Conférences et odirection de thèses

(*) Enseignant invité, associé, conférencier, ...

12- Partenaires : Accords et conventions nationaux et internationaux

(Joindre obligatoirement toutes les copies des conventions)

- ❖ **Convention de partenariat liant les établissements partenaires concerné par l'école doctorale :**
(Etablissements d'enseignement supérieur)
 - ✓ **Ecole doctorale régionale en Informatique 1 :**
 - ESI d'Alger,
 - Université Alger1,
 - Université de Bouira,
 - Université de Djelfa,
 - Université de Médéa,
 - Centre Universitaire d'Illizi,
 - Ecole Nationale des Technologies Avancées (ENSTA, Alger),
 - École supérieure en Sciences et Technologies de l'Informatique et du Numérique (ESTIN, Bejaia).
- ❖ **Convention de partenariat liant l'établissement au partenaire socio-économique, instances administratives, collectivités locales...etc**
(Conformément à la note n°242/SG/2024 du 28 février 2024)
 - ✓ **Agence Spatiale Algérienne « ASAL »**
 - ✓ **Entreprise LUNALOGIC SAS France**
 - ✓ **Watania Telecom Algérie « OOREDOO »**
 - ✓ **Huawei Telecommunications Algeria SARL**
 - ✓ **Institut National de Formation Supérieure Paramédicale de Béjaia à Aokas**
 - ✓ **Association des médecins généralistes libéraux de Béjaia**
 - ✓ **Forum de la cardiologie de Béjaia**
 - ✓ **La wilaya de Béjaia**
 - ✓ **CEVITAL(en cours)**
 - ✓ **DANONE (en cours)**
 - ✓ **Entreprise Portuaire de Béjaia - EPB**
- ❖ **Convention de partenariat liant l'établissement à un centre de recherche** (Conformément à la note n°242/SG/2024 du 28 février 2024)
 - ✓ **CERIST**
 - ✓ **Centre de Recherche en Langue et Culture Amazighes – CRLCA**
 - ✓ **Centre de Recherche en Technologies Agro-Alimentaires - CRTAA**
- ❖ **Autre**
 - Université de Béjaia
 - Université d'Eloued
 - Université de Béchar
 - Université Clermont Auvergne
 - Université du Québec en Outaouais – UQO
 - Grenoble INP – UGA
 - RMIT University - Australie

13- Structures d'adossement et de soutien à la formation :

❖ **Laboratoire de recherche :**

Dénomination du laboratoire	Directeur du laboratoire
Laboratoire d'Informatique et des Technologies Avancées du Numérique (LITAN) : C4460100	DJENADI Ali

❖ **Autres structures :**

Dénomination de la structure	Directeur/Responsable
Laboratoire d'Informatique Médicale : CO792300	SLIMANI Hachem
Unité de recherche en sciences des données et applications (CERIST)	BELAID Ahror

14- L'offre de formation doctorale fait-elle partie de la carte de formation de votre établissement ?

Oui ☒ Non ☐

Si oui joindre copie d'arrêtés.

**Modèle de CV à joindre pour tout participant à la Formation
(Une 1 page maximum)**

Nom et Prénom :	SEBAA Abderrazak
Dernier Diplôme et date d'obtention :	Habilitation Universitaire (2019)
Spécialité :	Informatique
Grade :	MCA
Fonction :	Enseignant chercheur
Etablissement de rattachement :	ESTIN Bejaia
Tel mobile	0550098094
Tel / Fax	
Mail	sebaa@estin.dz
Domaines scientifiques d'intérêts :	Informatique IA

Indiquer les 05 dernières publications :

"A Sebaa, N Djebari, A Tari", "Healthcare services: applications, trend, and challenges", 2024, "International Journal of Medical Engineering and Informatics 16 (10.1504 ...", "", "", "https://scholar.google.com", "21", "2024-05-21 19:52:28", "Journal article", "", "", "https://scholar.google.com/citations?view_op=view_citation&hl=en&user=9e-QMXYAAAAJ&pagesize=100&citation_for_view=9e-QMXYAAAAJ:L8Ckcd2t8MC", "", 0, 0.00, 0.3, 1, "", "", ""

"D Hadjout, A Sebaa, JF Torres, F Martínez-Álvarez", "Electricity consumption forecasting with outliers handling based on clustering and deep learning with application to the Algerian market", 2023, "Expert Systems with Applications", "", "", "https://scholar.google.com/scholar?oi=bibs&hl=en&cites=11714005162205356483", 10, "2024-05-21 19:52:28", "Journal article", "", "", "https://scholar.google.com/citations?view_op=view_citation&hl=en&user=9e-QMXYAAAAJ&pagesize=100&citation_for_view=9e-QMXYAAAAJ:TQgYirikUcIC", 227, 120123, 120123, 9, 9.00, 2, 4, 1, "", "", ""

"OS Mazari, A Sebaa, JL Amaro-Mellado, F Martínez-Álvarez", "Creating a homogenized earthquake catalog for Algeria and mapping the main seismic parameters using a geographic information system", 2023, "Journal of African Earth Sciences", "", "", "https://scholar.google.com/scholar?oi=bibs&hl=en&cites=10939796417911257515", 18, "2024-05-21 19:52:28", "Journal article", "", "", "https://scholar.google.com/citations?view_op=view_citation&hl=en&user=9e-QMXYAAAAJ&pagesize=100&citationfor_view=9e-QMXYAAAAJ:R3hNpaxXUuUC", 201, 104895, 104895, 1, 1.00, 0, 4, 1, "", "", ""

"D Azzougner, A Sebaa, D Hadjout, F Martínez-Álvarez", "Fraud detection of electricity consumption using robust exponential and holt-winters smoothing method", 2023, "2023 IEEE International Conference on Advanced Systems and Emergent ...", "", "", "https://scholar.google.com/scholar?oi=bibs&hl=en&cit es=8393063174818787182", 19, "2024-05-21 19:52:28", "Conference paper", "", "", "https://scholar.google.com/citations?view_op=view_citation &hl=en&user=9e-QMXYAAAAJ&pagesize=100&citation_for_view=9e-QMXYAAAAJ:e5wmG9Sq2KIC", "", 1, 1.00, 0, 4, 1, "", "", ""

"O Bentaleb, ASZ Belloum, A Sebba, A El-Maouhab","Containerization technologies: Taxonomies, applications and challenges",2022,"The Journal of Supercomputing",,,,,,"https://scholar.google.com/scholar?oi=bibs&hl=en&cite=9077267162213310278",2,"2024-05-21 19:52:28","Journal citation",,,,,,"https://scholar.google.com/citations?view_op=view_citation&hl=en&user=9e-QMXYAAAAJ&pagesize=100&citation_for_view=9e-QMXYAAAAJ:mVmsd5A6BfQC",78,1,1144,1181,69,34.50,17,4,2,,,,,""

Annexe n°1 : Modèle de CV à joindre pour tout participant à la Formation

(Une 1 page maximum)

Nom et Prénom : Elmir Youssef
Dernier Diplôme et date d'obtention : Habilitation Universitaire (2020)
Spécialité : Informatique
Grade : MCA
Fonction : Enseignant chercheur
Etablissement de rattachement : ESTIN
Tel mobile 0550447447
Tel / Fax
Mail elmir@estin.dz
Domaines scientifiques d'intérêts : Biometrics, Digital Health, Pattern Recognition, Machine Learning, Optimization
Indiquer les 05 dernières publications : Khennouche, Feriel; Elmir, Youssef; Himeur, Yassine; Djebari, Nabil; Amira, Abbas; Revolutionizing generative pre-trained: Insights and challenges in deploying ChatGPT and generative chatbots for FAQs, Expert Systems with Applications, 246, 123224, 2024, Elsevier
Khair, Younes; Dennai, Abdeslem; Elmir, Youssef; , Cloud-Based Demand-Responsive Transportation System Using Forecasting Model, Arabian Journal for Science and Engineering, 49, 3, 3829-3843, 2024, Springer Berlin Heidelberg Berlin/Heidelberg
Bechar, Amine; Elmir, Youssef; Medjoudj, Rafik; Himeur, Yassine; Amira, Abbas; , Harnessing transformers: A leap forward in lung cancer image detection, 2023 6th International Conference on Signal Processing and Information Security (ICSPIS), 218-223, 2023, IEEE
Elmir, Youssef; Laouar, Sid Ahmed; Hamdaoui, Larbi; , Transfer Learning-based Real-time Handgun Detection, arXiv preprint arXiv:2311.13559, 2023,
Melchane, Selestine; Elmir, Youssef; Kacimi, Farid; , Infectious Diseases Prediction Based On Machine Learning: The Impact Of Data Reduction Using Feature Extraction Techniques, HCist 2023 - International Conference on Health and Social Care Information Systems and Technologies, 2023,

Annexe n°1 : Modèle de CV à joindre pour tout participant à la Formation (Une 1 page maximum)

Nom et Prénom :	DJENADI Ali
Dernier Diplôme et date d'obtention :	Doctorat, 2021
Spécialité :	Electronique
Grade :	MCB
Fonction :	Enseignant-chercheur
Etablissement de rattachement :	École supérieure en sciences et technologies de l'informatique et du numérique
Tel mobile	0551962721
Tel / Fax	
Mail	djenadi@estin.dz
Domaines scientifiques d'intérêts :	Robotique ; intelligence artificielle ; Control des systèmes ; industrie 4.0
Indiquer les 05 dernières publications :	• Belaid A., Mendil B. and, Djenadi A. (2022) Narrow passage RRT*: A new variant of RRT*. International Journal of Computational Vision and Robotics. • Djenadi A. and Mendil B. (2021) Energy-aware task allocation strategy for multi robot system. International Journal of modeling and Simulation. • Djenadi A and Mendil B. Effect of tasks reallocation on the performance of a multi robot system in goods transportation. The Electrical Engineering International Conference EEIC'19. 4,5 December 2019, Bejaia, Algerie

Annexe n°1 : Modèle de CV à joindre pour tout participant à la Formation

(Une 1 page maximum)

Nom et Prénom : TARI Abdelkamel
Dernier Diplôme et date d'obtention : Doctorat
Spécialité : Informatique
Grade : Professeur
Fonction : Enseignant chercheur
Etablissement de rattachement : ESTIN
Tel mobile 0550658892
Tel / Fax
Mail tari@estin.dz
Domaines scientifiques d'intérêts : Data Mining, Apprentissage automatique, Optimisation des systèmes, Systèmes distribués.

Indiquer les 05 dernières publications :

"S Hameche, ME Khanouche, A Chibani, A Tari", "A Group Teaching Optimization-Based Approach for Energy and QoS-Aware Internet of Things Services Composition", 2024, "Journal of Network and Systems Management", "", "", "https://scholar.google.com/scholar?oi=bibs&hl=en&cites=10875970947116473485", 88, "2024-05-21 19:58:58", "Journal article", "", "", "https://scholar.google.com/citations?view_op=view_citation&hl=en&user=7LyPCJIAAAAJ&pagesize=100&citation_for_view=7LyPCJIAAAJ:g3aElNc5_aQC", 32, 1, 4, 4, 1, 1.00, 0, 4, 1, "", "", ""

"A Dabba, A Tari, S Meftali", "A novel grey wolf optimization algorithm based on geometric transformations for gene selection and cancer classification", 2024, "The Journal of Supercomputing", "", "", "https://scholar.google.com/scholar?oi=bibs&hl=en&cites=778182994321262649", 89, "2024-05-21 19:58:58", "Journal article", "", "", "https://scholar.google.com/citations?view_op=view_citation&hl=en&user=7LyPCJIAAAAJ&pagesize=100&citation_for_view=7LyPCJIAAAJ:hMsQuOkut0C", 80, 4, 4808, 4840, 1, 1.00, 0, 3, 1, "", "", ""

"S Hameche, ME Khanouche, A Tari", "Mobility and energy efficient services composition algorithm with QoS guarantee for large scale Cyber-Physical-Social Systems", 2024, "Expert Systems with Applications", "", "", "https://scholar.google.com", 98, "2024-05-21 19:58:58", "Journal article", "", "", "https://scholar.google.com/citations?view_op=view_citation&hl=en&user=7LyPCJIAAAAJ&pagesize=100&citation_for_view=7LyPCJIAAAJ:kuK5TVdYjLIC", 249, 123683, 123683, 0, 0.00, 0, 3, 1, "", "", ""

"S Ait Hacène Ouhadda, S Chibani Sadouki, A Achroufene, A Tari", "A Discrete Adaptive Lion Optimization Algorithm for QoS-Driven IoT Service Composition with Global Constraints", 2024, "Journal of Network and Systems Management", "", "", "https://scholar.google.com", 99, "2024-05-21 19:58:58", "Journal article", "", "", "https://scholar.google.com/citations?view_op=view_citation&hl=en&user=7LyPCJIAAAAJ&pagesize=100&citation_for_view=7LyPCJIAAAJ:gsN89kCJA0AC", 32, 2, 34, 34, 0, 0.00, 0, 4, 1, "", "", ""

"A Sebaa, N Djebbari, A Tari", "Healthcare services: applications, trend, and challenges", 2024, "International Journal of Medical Engineering and Informatics", "", "", "https://scholar.google.com", 100, "2024-05-21 19:58:58", "Journal article", "", "", "https://scholar.google.com/citations?view_op=view_citation&hl=en&user=7LyPCJIAAAAJ&pagesize=100&citation_for_view=7LyPCJIAAAJ:TIZ-Mc8IILK0C", 16, 2, 161, 172, 0, 0.00, 0, 3, 1, "", "", ""

Annexe n°1 : Modèle de CV à joindre pour tout participant à la Formation

(Une 1 page maximum)

Nom et Prénom : KHANOUCHE Mohamed Essaid
Dernier Diplôme et date d'obtention : Doctorat
Spécialité : Informatique
Grade : MCA
Fonction : Enseignant chercheur
Etablissement de rattachement : ESTIN
Tel mobile 0550658892
Tel / Fax
Mail khanouche@estin.dz
Domaines scientifiques d'intérêts : IA

Indiquer les 05 dernières publications :

S. Hameche, M. E. Khanouche, and A. Tari, "Mobility and energy efficient services composition algorithm with QoS guarantee for large scale Cyber-Physical-Social Systems," Expert Systems with Applications, vol. 249, Part C (123683), March 2024.

S. M. Hammoum, M. E. Khanouche, N. Khoulalene and B. Benatallah, "Uncertainty QoS-aware Services Composition: A Systematic Literature Review for Services Community," Service Oriented Computing and Applications, DOI: 10.1007/s11761-024-00389-9, March 2024.

S. Hameche, M. E. Khanouche, A. Chibani and A. Tari, "A group teaching optimization-based approach for energy and QoS-aware Internet of Things services composition," J. Net. and Sys. Management, 32: 4, 2024.

A. Cherifi, M. E. Khanouche, Y. Amirat and Z. Farah, "A parallel approach for user-centred QoS-aware services composition in the Internet of Things," Eng. App. of Art. Intelligence, vol. 123, Part B, 106277, 2023.

A. Kouicem, M. E. Khanouche and A. Tari, "Novel bat algorithm for QoS-aware services composition in large scale Internet of Things," Cluster Computing, vol. 25, pp. 3683–3697, 2022.

P. Alizadeh, A. Osmani, M. E. Khanouche, A. Chibani and Y. Amirat, "Reinforcement Learning for Interactive QoS-Aware Services Composition," IEEE Systems J., vol. 15, no 1, pp. 1098–1108, 2021.

N. Kadjouh, A. Bounceur, M. Bezoui, M. E. Khanouche, R. Euler, M. Hammoudeh, L. Lagadec, S. Jabbar and F. Al-Turjman, "A Dominating Tree based Leader Election Algorithm for Smart Cities IoT Infrastructure," Mobile Networks and Applications (Springer), vol. 28, pp. 718–731, 2020.

M. E. Khanouche, N. Atmani and A. Cherifi, "Improved Teaching Learning-based QoS-aware services composition for Internet of Things," IEEE Systems J., vol. 14, no. 3, pp. 4155–4164, 2020.

M. E. Khanouche, H. Gadouche, F. Zoubeyr and A. Tari, "Flexible QoS-aware services composition for Service Computing environments," Computer Networks, vol. 166, pp. 106982:1, 106982:12, 2020.

Mohamed Arbane, Mohamed Essaid Khanouche, Ghazaleh Khodabandelou, Abdelghani Chibani and Yacine Amirat, "DRSU-net: Depth-Residual Separable U-net model for Semantic Segmentation," International Joint Conference on Neural Networks (IJCNN), Gold Coast, Australia, pp. 1-6, Jun 2023.

Laldja Ziani, Mohamed Essaid Khanouche and Ahror Belaid, "Internet of Behaviors : A literature review of an emerging technology," International Conference on Big data, IoT, Web intelligence and Applications, Sidi Bel Abbès, Algeria, 10:1–10:6, December, 2022.

Annexe n°1 : Modèle de CV à joindre pour tout participant à la Formation

(Une 1 page maximum)

Nom et Prénom : FARAH ZOubeyr
Dernier Diplôme et date d'obtention : Doctorat en Sciences
Spécialité : Informatique
Grade : MCA
Fonction : Enseignant chercheur
Etablissement de rattachement : Université de bejaia
Tel mobile 0556838958
Tel / Fax
Mail farah@estin.dz
Domaines scientifiques d'intérêts : Sécurité Informatique, Validation formelle, architectures orientées services, algorithmes bio-inspirés, Intelligence artificielle.

Indiquer les 05 dernières publications : Asma Cherifi, Mohamed Essaid Khanouche, Yacine Amirat, Zoubeyr Farah, A parallel approach for user-centered QoS-aware services composition in the Internet of Things, Engineering Applications of Artificial Intelligence, Volume 123, Part B, 2023, 106277,ISSN 0952-1976, <https://doi.org/10.1016/j.engappai.2023.106277>.

Khanouche, Mohamed Essaid, Hania Gadouche, Zoubeyr Farah, and Abdelkamel Tari. "Flexible QoS-aware services composition for service computing environments." Computer Networks 166 (2020): 106982.

Gadouche, Hania, Zoubeyr Farah, and Abdelkamel Tari. "A Valid and Correct-by-Construction Formal Specification of RBAC." International Journal of Information Security and Privacy (IJISP) 14, no. 2 (2020): 41-61.

Farah Zoubeyr, Hania Gadouche, Abdelkamel Tari: A Correct-by-Construction Model for Attribute-Based Access Control. MEDI 2018: 233-247.

Farah Zoubeyr, Hania Gadouche, Abdelkamel Tari: A correct-by-construction model for attribute-based access control. Cluster Comput (2019). <https://doi.org/10.1007/s10586-019-02976-4>.

Annexe n°1 : Modèle de CV à joindre pour tout participant à la Formation (Une 1 page maximum)

Nom et Prénom : Azouaou Faical
Dernier Diplôme et date d'obtention : Doctorat
Spécialité : Informatique
Grade : Professeur
Fonction : Enseignant chercheur
Etablissement de rattachement : ESTIN
Tel mobile 0561270101
Tel / Fax
Mail azouaou@estin.dz
Domaines scientifiques d'intérêts : nlp, lawtech, technology enhanced learning, social mining
Indiquer les 05 dernières publications :

Guellil, Imane; Azouaou, Faical; Chiclana, Francisco;
 ArAutoSenti: automatic annotation and new
 tendencies for sentiment classification of Arabic messages
 Social Network Analysis and Mining 10
 1-20 2020 Springer Vienna

Guellil, Imane; Azouaou, Faical; Benali, Fodil; Hachani, Ala
 Eddine; Mendoza, Marcelo; The role of
 transliteration in the process of arabizi
 translation/sentiment analysis Recent Advances in NLP:
 The Case of Arabic Language 101-128
 2020 Springer International Publishing

Guellil, Imane; Mendoza, Marcelo; Azouaou, Faical;
 Arabic dialect sentiment analysis with ZERO
 effort.\\Case study: Algerian dialect Inteligencia
 Artificial 23 65 124-135 2020

Guellil, Imane; Saâdane, Houda; Azouaou, Faical; Gueni,
 Billel; Nouvel, Damien; Arabic natural language
 processing: An overview Journal of King Saud University-
 Computer and Information Sciences 33 5
 497-507 2021 Elsevier

Guellil, Imane; Adeel, Ahsan; Azouaou, Faical; Chennoufi,
 Sara; Maafi, Hanene; Hamitouche, Thinhinane;
 Detecting hate speech against politicians in Arabic
 community on social media International Journal of
 Web Information Systems 16 3 295-313
 2020 Emerald Publishing Limited

Annexe n°1 : Modèle de CV à joindre pour tout participant à la Formation

(Une 1 page maximum)

Nom et Prénom : DENNAI Abdeslem
Dernier Diplôme et date d'obtention : HDR - 08/01/2017
Spécialité : Informatique
Grade : Professeur
Fonction : Enseignant chercheur
Etablissement de rattachement : Université TAHRI Mohammed BECHAR
Tel mobile 0676390095
Tel / Fax 044636232
Mail dennai.abdeslam@univ-bechar.dz
Domaines scientifiques d'intérêts : E-Health et traitement des données médicales, les environnements Cloud, Fog et Edge Computing.

Indiquer les 05 dernières publications :

- 1- <https://link.springer.com/journal/11227/volumes-and-issues/78-17>
- 2- <https://doi.org/10.1093/comjnl/bxad001>
- 3- <https://www.tobreg.org/index.php/journal/article/view/1562>
- 4- <https://worldscientific.com/doi/10.1142/S0219649222500563>
- 5- <https://worldscientific.com/doi/10.1142/S0219649222500824>
- 6- <https://www.math.md/publications/csjm/issues/v31-n1/13652/>
- 7- <https://link.springer.com/article/10.1007/s13369-023-08102-2>
- 8- <https://www.dline.info/jitr/v10n3.php>
- 9- https://link.springer.com/chapter/10.1007/978-3-030-37207-1_7
- 10- <https://dl.acm.org/doi/proceedings/10.1145/3384544>
- 11- https://link.springer.com/chapter/10.1007/978-3-030-63846-7_53
- 12- https://link.springer.com/chapter/10.1007/978-981-16-5207-3_6
- 13- https://link.springer.com/chapter/10.1007/978-3-030-92038-8_45
- 14- https://link.springer.com/chapter/10.1007/978-3-030-96311-8_36

Annexe n°1 : Modèle de CV à joindre pour tout participant à la Formation (Une 1 page maximum)

Nom et Prénom :	Belaid Ahror
Dernier Diplôme et date d'obtention :	Doctorat
Spécialité :	Informatique
Grade :	Professeur
Fonction :	Enseignant Chercheur
Etablissement de rattachement :	CERIST
Tel mobile	0555611741
Tel / Fax	
Mail	belaid@estin.dz
Domaines scientifiques d'intérêts :	Intelligence artificielle
Indiquer les 05 dernières publications :	Cross-dimensional transfer learning in medical image segmentation with deep learning H Messaoudi, A Belaid, DB Salem, PH Conze Medical image analysis 88, 102868, 2023 Convolutional neural networks-based method for skin hydration measurements in high resolution MRI R Zegour, A Belaid, J Ognard, DB Salem Biomedical Signal Processing and Control 81, 10449, 2023 Efficient embedding network for 3D brain tumor segmentation H Messaoudi, A Belaid, ML Allaoui, A Zetout, MS Allili, S Tliba, ... Brainlesion: Glioma, Multiple Sclerosis, Stroke and Traumatic Brain Injuries, 2021 Automatic Forensic Identification using 3D Sphenoid Sinus Segmentation and Deep Characterization K Souadih, A Belaid, DB Salem, PH Conze Medical & Biological Engineering & Computing 58, 291–306, 2020

Annexe n°2 : Objectifs assignés à la formation doctorale

✓ Objectifs :

- Contribuer à la réalisation des objectifs prioritaires socio-économiques du pays :
 - Mettre l'accent sur le développement de nouveaux modèles et techniques d'intelligence artificielle adaptés aux défis socio-économiques, tels que la sécurité alimentaire, l'efficacité énergétique et la promotion de la santé et du bien-être citoyen.
 - Identifier les applications potentielles de l'intelligence artificielle dans des domaines spécifiques comme l'agriculture intelligente, la gestion des ressources énergétiques et la santé publique.
- Fédérer et consolider les connaissances acquises dans les parcours actuels de Master :
 - Intégrer les enseignements et les avancées de la recherche doctorale dans les cursus de Master existants, notamment dans les domaines de l'intelligence artificielle, de la cybersécurité et de la science des données.
 - Assurer la qualité des enseignements en intégrant des modules ciblés sur les applications pratiques de l'intelligence artificielle dans les domaines prioritaires.
- Offrir une formation académique de haut niveau pour les futurs enseignants-chercheurs :
 - Promouvoir la formation par la recherche en permettant aux doctorants d'acquérir des compétences approfondies dans des domaines clés de l'informatique, en mettant l'accent sur les applications de l'intelligence artificielle dans des contextes réels.
- Favoriser la formation pluridisciplinaire dans les technologies de l'informatique :
 - Encourager une approche pluridisciplinaire en intégrant des modules sur les technologies émergentes telles que l'intelligence artificielle, les sciences des données, la cybersécurité et l'internet des objets/des comportements.
 - Préparer les futurs enseignants-chercheurs à répondre aux besoins en matière de formation dans ces spécialités émergentes, afin de soutenir l'innovation et le développement économique du pays.
- Former des chercheurs capables de mettre en œuvre des solutions adaptées au marché de l'emploi :
 - Mettre l'accent sur la formation pratique et la collaboration avec l'industrie pour développer des compétences qui répondent aux besoins du marché de l'emploi dans des domaines spécifiques, en mettant en avant les applications de l'intelligence artificielle dans les secteurs prioritaires.
- Satisfaire les besoins des acteurs économiques nationaux dans le cadre des politiques de sécurité en matière de développement national des systèmes intelligents :

- Explorer les implications de la sécurité et de la confidentialité des données dans le déploiement de systèmes intelligents dans les secteurs prioritaires, en mettant l'accent sur les défis liés à la protection des données personnelles dans les domaines de la santé, de l'énergie et de la sécurité alimentaire.
- Collaborer avec les acteurs économiques nationaux pour identifier les besoins spécifiques en matière de développement de systèmes intelligents et concevoir des solutions adaptées, en utilisant les techniques avancées de l'intelligence artificielle et de la science des données.

✓ **Le lien entre les projets proposés :**

Cette formation doctorale présente un lien étroit avec les axes de recherche stratégiques et prioritaires, notamment la sécurité alimentaire, la sécurité énergétique, et la santé du citoyen et son bien-être, de la manière suivante :

1. Sécurité Alimentaire :

- Les techniques d'intelligence artificielle peuvent être appliquées à l'agriculture intelligente pour optimiser la production agricole, la gestion des ressources naturelles et la prévention des maladies des cultures.
- Les doctorants peuvent se concentrer sur le développement de modèles prédictifs pour anticiper les rendements agricoles, identifier les maladies des plantes et optimiser l'utilisation des ressources telles que l'eau et les engrais, contribuant ainsi à la sécurité alimentaire nationale.

2. Sécurité Énergétique :

- L'intelligence artificielle peut être utilisée pour améliorer l'efficacité énergétique, optimiser la distribution et la consommation d'énergie, et promouvoir l'utilisation de sources d'énergie renouvelables.
- Les doctorants peuvent explorer des domaines tels que la prédiction de la demande énergétique, l'optimisation des réseaux électriques intelligents, et la détection des anomalies dans les infrastructures énergétiques, contribuant ainsi à renforcer la sécurité et la stabilité du réseau énergétique national.

3. Santé du Citoyen et Bien-être :

- Les applications de l'intelligence artificielle dans le domaine de la santé peuvent inclure le diagnostic médical assisté par ordinateur, la personnalisation des traitements médicaux, et la surveillance de la santé à domicile.
- Les doctorants peuvent se concentrer sur le développement de modèles de prédiction des maladies, l'analyse des données médicales pour identifier les tendances et les facteurs de risque, et la création de systèmes d'aide à la décision pour les professionnels de la santé, contribuant ainsi à améliorer la santé et le bien-être des citoyens.

Annexe n°3 : Les capacités effectives

✓ Compétences humaines mobilisées :

Cette formation doctorale mobilise un ensemble diversifié et dynamique de compétences humaines pour offrir un environnement d'apprentissage et de recherche de qualité. Avec (05) cinq enseignants-chercheurs habilités (PR & MCA) en informatique à l'ESTIN, la formation bénéficie d'une expertise solide et variée dans les domaines de l'intelligence artificielle, des sciences des données et de la cybersécurité. En outre, sept (07) docteurs (MCB) en informatique, deux (02) enseignants chercheurs en électronique et en recherche opérationnelle ainsi que deux (02) enseignants-chercheurs retraités (Pr), renforcent davantage le programme en apportant des perspectives innovantes et une expérience approfondie de la recherche académique. Cette expertise est complétée par la participation active de professeurs, enseignants-chercheurs et chercheurs algériens à l'étranger, notamment ceux des universités renommées telles que l'Université Clermont Auvergne, l'Université du Québec en Outaouais, l'Université de Berlin, l'Université de Sharjah, l'Université de Dubai, l'Université Lyon 1 et l'Université Paris Cergy ...etc. De plus, les collaborations avec des établissements nationaux tels que l'Université de Béjaia, l'Université de Béchar, l'Université d'El Oued et le Centre de Recherche sur l'Information Scientifique et Technique (CERIST) enrichissent le programme en favorisant des échanges de connaissances et une recherche collaborative axée sur les priorités nationales en matière de sécurité alimentaire, de sécurité énergétique et de santé du citoyen.

✓ Moyens matériels déployés :

En plus des équipements des deux laboratoires d'adossement (LITAN & LIMED), cette formation dispose d'une infrastructure matérielle robuste pour soutenir les travaux de recherche et de développement en informatique et en intelligence artificielle. Cela comprend l'acquisition de PC puissants pour les doctorants ainsi qu'un datacenter doté d'une architecture informatique performante, hyperconvergente, modulable, évolutive et flexible. Ce datacenter offre une plateforme de calcul haute performance (CPU & GPU) pour développer et entraîner des modèles d'intelligence artificielle, ainsi qu'une infrastructure HCI pour héberger les serveurs de production et les applications métiers de l'école. En outre, une station de travail Z8 G4 équipée de composants haut de gamme sont fournies pour les travaux d'IA. En complément, des plateformes de développement Raspberry Pi 4 sont mises à disposition, offrant un environnement flexible et abordable pour expérimenter et développer des projets dans divers domaines de l'informatique, y compris l'IA, l'IoT et l'Edge Computing.

Annexe n°4 : Plan de recherche 1

Exploring transferability of explanations in Machine Learning

✓ Contexte de recherche :

The transferability of explanations refers to the extent to which interpretability or justification for the decision-making processes of one machine learning model can be effectively applied to another model, potentially of a different type or trained on different data. This research explores the challenges and opportunities in transferring explanations between models, investigating the conditions under which explanations remain valid and informative across diverse machine-learning settings. The research on the transferability of explanations in machine learning aims to unravel the intricacies involved in applying interpretability and justifications from one model to another. In addressing this complex challenge, one key aspect is navigating the heterogeneity among models, considering

scenarios where explanations developed for interpretable models may need to be transferred to more complex, black-box models. Another critical challenge involves understanding how explanations fare across varying data distributions, delving into the impact of shifts in data characteristics on the reliability of transferred explanations. Furthermore, the study examines the nuances of feature relevance across different domains, assessing the interpretability of model decisions when transferred across disparate problem spaces. Beyond model-centric challenges, the research delves into the robustness of transferred explanations under perturbations and the intricacies of transferring explanations within ensemble models. The anticipated outcomes of this research include valuable insights into the conditions under which explanations can be effectively transferred, contributing guidelines for practitioners and researchers to enhance the interpretability and trustworthiness of machine learning models in various contexts. This involves understanding the factors that influence the transferability of explanations, evaluating the reliability and robustness of explanations when applied to different models or datasets, and identifying scenarios where transferability may be particularly challenging or beneficial. The research will contribute insights into the practical implications of using explanation techniques in diverse machine-learning applications.

✓ Résumé et mots clés :

Machine Learning, XAI, Transfert learning

Annexe n°4 : Plan de recherche 2

Enhancing Chatbot Performance with Large Language Models (LLMs)

✓ Contexte de recherche :

- To evaluate the performance of state-of-the-art LLMs in chatbot applications.
- To implement LLMs in various chatbot frameworks and assess improvements in contextual understanding and response generation.
- To measure the impact of LLM-enhanced chatbots on user satisfaction and engagement.
- To identify and address challenges associated with the integration of LLMs in chatbot systems.

Methodology

Literature Review

A comprehensive review of existing literature on LLMs, their applications, and limitations in chatbot systems will be conducted. Key references include Hadi et al. (2023), which provides an extensive survey of LLM applications and challenges.

Evaluation of Current LLMs

State-of-the-art LLMs, such as GPT-4 and Gemini, will be evaluated based on their performance in generating contextually relevant and accurate responses. Metrics for evaluation will include response accuracy, coherence, and contextual understanding.

Implementation and Testing

The selected LLMs will be integrated into various chatbot frameworks. Testing will involve real-world conversational scenarios to assess improvements in chatbot performance. User feedback will be collected to gauge satisfaction and engagement levels.

Impact Assessment

The impact of LLM-enhanced chatbots on user interaction will be measured using quantitative metrics (e.g., response time, error rate) and qualitative feedback (e.g., user satisfaction surveys).

Expected Contributions

- Enhanced performance and user experience in chatbot interactions through the application of LLMs.
- Insights into the challenges and solutions associated with integrating LLMs in chatbot systems.
- Recommendations for future research and development in the field of AI-driven conversational agents.

Reference

Hadi, M. U., Qureshi, R., Shah, A., Irfan, M., Zafar, A., Shaikh, M. B., ... & Mirjalili, S. (2023). Large language models: a comprehensive survey of its applications, challenges, limitations, and future prospects. Authorea Preprints.

✓ Résumé et mots clés :

This thesis explores the application of Large Language Models (LLMs) to improve the performance, accuracy, and user interaction experience of chatbots. By leveraging the advanced capabilities of LLMs, such as GPT-4 and Gemini, this research addresses common limitations in traditional chatbot systems, including contextual understanding, response generation, and adaptability to diverse conversational scenarios. The study involves a comprehensive evaluation of current LLMs, implementation of these models in various chatbot frameworks, and assessment of their impact on user satisfaction and engagement.

Annexe n°4 : Plan de recherche 3

Développement d'interfaces homme-robot intuitives basées sur des approches neuro-symboliques pour une communication et une collaboration efficaces entre les humains et les cobots dans les environnements médicaux.

✓ Contexte de recherche :

Avec l'avènement de la santé 4.0, L'introduction des cobots (robots collaboratifs) dans les environnements médicaux (ex : hôpitaux, centre de soins, laboratoire d'analyse) offre de nouvelles opportunités pour améliorer les processus cliniques et la qualité des soins. Cependant, pour garantir des interactions sûres et efficaces entre les cobots et le personnel médical ainsi qu'avec les patients, il est essentiel que les robots communiquent efficacement et expliquent leurs raisonnements et actions dans les divers contextes de soins de santé. Les approches neuro-symboliques offrent une solution convaincante en combinant les forces du raisonnement symbolique avec les capacités d'apprentissage des réseaux neuronaux. Ces approches pourraient contribuer à renforcer la sécurité, l'adaptabilité et l'intelligence des cobots, permettant ainsi une collaboration plus étroite avec le personnel médical dans divers contextes de soins de santé.

✓ Résumé et mots clés :

Résumé:

Cette recherche vise à explorer l'application des approches neuro-symboliques aux cobots (robots collaboratifs) dans les environnements médicaux. En combinant les atouts du raisonnement symbolique et des capacités d'apprentissage des réseaux neuronaux, ces approches permettent aux cobots de prendre des décisions éclairées basées sur des schémas appris et de fournir des explications compréhensibles fondées sur des représentations logiques. L'intégration de ces approches permettra d'adapter les cobots pour assister le personnel médical dans des tâches telles que, le transport de matériel médical, l'assistance aux procédures chirurgicales ou la fourniture de soins aux patients. Ce projet vise à développer des cobots intelligents et adaptables qui peuvent optimiser les processus cliniques en veillant à la sécurité et au bien-être des patients.

Mots Clés: Cobots, Santé, Approches Neuro-Symboliques, Sécurité des Patients, Assistance Médicale, Collaboration Robot-Humain.

Annexe n°4 : Plan de recherche 4

Intégration Multimodale d'Images 2D et de Nuages de Points 3D pour une Classification d'Images Plus Précise : Application à la Classification d'Images d'Herbiers

✓ Contexte de recherche :

La classification d'images est un domaine essentiel de la vision par ordinateur, ayant des implications cruciales dans divers domaines, de la reconnaissance faciale à l'analyse de données médicales. Toutefois, les performances des modèles de classification d'images en deep learning peuvent être sérieusement compromises dans des situations où les images présentent un niveau significatif de bruit visuel. Les raisons de cette dégradation de performance sont multiples : le bruit visuel peut altérer les caractéristiques cruciales de l'image utilisées par le modèle pour la classification, rendre les images plus similaires entre différentes classes, et même induire un surapprentissage en présence de données d'entraînement bruitées. De nombreuses techniques ont été proposées pour résoudre ce problème, allant de l'utilisation de modèles plus robustes à l'amélioration des techniques de prétraitement et d'augmentation des données. Cependant, la qualité des images d'entraînement reste un facteur clé dans la performance des modèles.

Une avancée significative dans ce domaine réside dans l'intégration de données tridimensionnelles, telles que les nuages de points, dans les architectures de deep learning destinées à la classification d'images 2D. Les modèles de deep learning qui traitent des images 2D et ceux qui manipulent des données 3D sous forme de nuages de points diffèrent fondamentalement dans les caractéristiques qu'ils apprennent. Les modèles d'images 2D se focalisent sur des caractéristiques visuelles telles que les bords, les textures et les motifs, tandis que les modèles 3D s'attachent davantage à la structure tridimensionnelle, aux distances spatiales et aux relations entre les points. La fusion de ces deux types de données peut être complémentaire, car elles capturent des aspects différents de l'environnement. Par exemple, en combinant des images 2D avec des nuages de points 3D, les modèles peuvent mieux appréhender la géométrie tridimensionnelle d'une scène tout en utilisant les informations visuelles pour enrichir la sémantique de la classification ou de la segmentation. Cette approche combinée peut considérablement améliorer les performances des modèles de deep learning en offrant une compréhension plus complète et précise de l'environnement par rapport à l'utilisation exclusive de l'une ou l'autre source de données.

Ainsi, ce sujet de thèse vise à explorer et à développer une architecture de deep learning innovante qui fusionne de manière efficace les données 2D et 3D pour améliorer la précision et l'efficacité de la classification d'images.

L'utilisation spécifique de la classification d'images d'herbier illustre parfaitement l'importance de la fusion des données 2D et 3D en deep learning. Lors de la classification de spécimens botaniques à partir d'images, les modèles basés uniquement sur des images 2D peuvent être limités, car ils ont du mal à distinguer des espèces similaires avec des variations subtiles dans leur apparence visuelle. L'intégration de données 3D sous forme de nuages de points permet aux modèles de saisir la structure tridimensionnelle des plantes, incluant la disposition des feuilles, la forme des tiges, et d'autres caractéristiques cruciales pour une classification précise.

Objectifs de la thèse :

1. Étudier et évaluer les algorithmes existants de segmentation d'image et de reconnaissance de forme dans le contexte des images 2D et 3D.
2. Proposition d'une approche de fusion multimodal, combinant à la fois les images 2D et les images 3D (nuages de points), pour la classification des images 2D. Application de l'approche pour la reconnaissance de traits sur les images d'herbier.
3. Évaluer l'efficacité des méthodes développées en termes de précision, de rappel et de pertinence pour les utilisateurs finaux.

Méthodologie :

La recherche impliquera une analyse critique des méthodes existantes et le développement de nouvelles techniques optimisées pour la caractérisation 3D et 2D. Des approches expérimentales et computationnelles seront utilisées pour tester et valider les algorithmes développés. Les résultats seront évalués quant à leur capacité à améliorer l'accès et la manipulation des données des collections d'herbiers numérisées.

Plan:

Année 1 : Fondements et Collecte de Données

- Revue approfondie de la littérature sur la classification d'images en deep learning et les problèmes liés au bruit visuel.
- Définition claire de la problématique et des objectifs de recherche.
- Collecte et prétraitement des données d'entraînement (images 2D et nuages de points 3D) pour les expériences.
- Conception préliminaire de l'architecture de fusion des données 2D et 3D.
- Début de l'expérimentation avec des modèles de base.

Année 2 : Développement avancé des Modèles et Expérimentation

- Affinement de l'architecture de fusion des données 2D et 3D en fonction des premiers résultats.
- Expansion de l'expérimentation sur des ensembles de données plus vastes et diversifiés.
- Entraînement en profondeur des modèles en utilisant des techniques d'optimisation avancées.
- Analyse approfondie des caractéristiques apprises et identification des points forts et faibles.
- Rédaction d'articles pour des conférences et des revues académiques.

Année 3 : Évaluation, Validation et Rédaction de Thèse

- Évaluation quantitative des performances des modèles sur des ensembles de données de test.
- Étude de cas spécifique : Classification d'images d'herbier pour illustrer l'impact de la fusion 2D-3D.
- Comparaison des résultats avec les modèles basés uniquement sur des données 2D.
- Rédaction de la thèse.

Bibliographie :

- Olivier Pradelle, Raphaëlle Chaine, David Wendland, and Julie Digne. 2023. Light- weight integration of 3D features to improve 2D image segmentation. *Computers Graphics* 114 (2023).
- R. Charles, H. Su, M. Kaichun, and L. J. Guibas. 2017. PointNet: Deep Learning on Point Sets for 3D Classification and Segmentation. In 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR).
- Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. 2015. Deep Residual Learning for Image Recognition. arXiv:1512.03385 [cs.CV]
- Jianghong Zhao, Yinrui Wang, Yue Cao, Ming Guo, Xianfeng Huang, Ruiju Zhang, Xintong Dou, Xinyu Niu, Yuanyuan Cui, and Jun Wang. 2021. The Fusion Strategy of 2D and 3D Information Based on Deep Learning: A Review. *Remote Sensing* 13, 20 (2021). <https://doi.org/10.3390/rs13204029>
- Alec Radford, Jong Wook Kim, Chris Hallacy, Aditya Ramesh, Gabriel Goh, Sandhini Agarwal, Girish Sastry, Amanda Askell, Pamela Mishkin, Jack Clark, Gretchen Krueger, and Ilya Sutskever. 2021. Learning Transferable Visual Models From Natural Language Supervision, ICML 2021,
- Walid Mahdi Abdelaziz Triki, Bassem Bouaziz. 2022. A deep learning-based approach for detecting plant organs from digitized herbarium specimen images. *Ecological Informatics* 69 69 (2022), 1–7. <https://doi.org/10.1016/j.ecoinf.2022.101590>

✓ Résumé et mots clés :

Annexe n°4 : Plan de recherche 5

Enhancing Explainability and Interpretability of Deep Learning Models for Security Applications

✓ Contexte de recherche :

Deep learning models have revolutionized computer vision tasks, achieving impressive performance in areas like object detection, facial recognition, and anomaly detection. However, their widespread adoption in security applications is hampered by a lack of explainability and interpretability. These models often function as "black boxes," where the internal decision-making process remains opaque. This opacity can lead to several challenges:

- **Limited Trust and Transparency:** Security personnel and stakeholders might struggle to trust model decisions without understanding the underlying rationale. This can hinder adoption and raise concerns about accountability.
- **Difficulty in Debugging and Improvement:** When a model makes a security-critical error, it's challenging to pinpoint the root cause and identify areas for improvement without understanding how the model arrived at its decision.
- **Potential for Bias and Discrimination:** Deep learning models trained on biased data can perpetuate those biases in their outputs. Explainability techniques can help identify and mitigate such biases in security contexts.

✓ Résumé et mots clés :

This thesis proposes to investigate and develop methods for enhancing the explainability and interpretability of deep learning models used in security applications. By shedding light on the internal workings of these models, the research aims to:

Increase trust and transparency in security decisions made by deep learning models.

Facilitate debugging and improvement of the models, allowing for faster and more targeted interventions when errors occur.

Help identify and mitigate potential biases within the models, ensuring fairer and more reliable security outcomes.

Keywords : Deep learning, Explainable AI (XAI), Interpretable machine learning, Computer vision security, Adversarial attacks, Model bias, Security applications, Object detection, Facial recognition, Anomaly detection

Annexe n°4 : Plan de recherche 6

Analyzing the Psychological Consequences of Intrusion and Manipulation in Recommender Systems for Fake Recommendations Distribution

✓ Contexte de recherche :

Recommender systems play a crucial role in shaping the information and content consumed by users on social media and web applications. However, these systems are vulnerable to intrusion and manipulation by malicious actors, who may exploit them to distribute fake or biased recommendations. The psychological impact of such intrusions on users' stress levels, anxiety, and overall mental well-being is a significant concern that requires thorough investigation.

Résumé et mots clés :

The thesis subject focuses on analyzing the psychological consequences of intrusion and manipulation in recommender systems for the distribution of fake recommendations. It aims to investigate the potential attack vectors and vulnerabilities in recommender systems that enable the injection of fake or biased recommendations, and to develop techniques for simulating and analyzing such scenarios.

The research objectives include analyzing the propagation and psychological impacts of consuming fake or manipulated recommendations, exploring the potential long-term psychological effects of prolonged exposure to such recommendations, and developing strategies for detecting and mitigating the spread of fake or biased recommendations.

Additionally, the research aims to define health status indicators and metrics to assess the psychological well-being of users affected by fake or biased recommendations, considering factors such as increased stress levels, anxiety, cognitive dissonance, and the erosion of trust in information sources.

The methodology involves a combination of technical approaches, such as adversarial machine learning and data poisoning, as well as psychological approaches, including user studies, surveys, and psychological assessments. The expected contributions include identifying vulnerabilities and proposing mitigation strategies for secure and trustworthy recommender systems, providing insights into the psychological consequences of such intrusions, and developing interventions and support mechanisms to protect users from negative psychological impacts.

key words: Recommender Systems, Intrusion, Manipulation, Fake Recommendations, Psychological Consequences

Annexe n°4 : Plan de recherche 7

Modèles de Transformers pour le diagnostic des troubles dépressifs à partir des données Électroencéphalogrammes

✓ **Contexte de recherche :**

✓ **Résumé et mots clés :**

La dépression est une maladie psychologique fréquente qui perturbe fortement la vie quotidienne. L'étude des activités cérébrales via l'électroencéphalographie (EEG) peut être exploré pour détecter les troubles dépressifs chez un patient [1][2].

Les progrès récents dans les techniques d'apprentissage profond et en particulier les Transformers (appelé aussi modèle auto-attention) [3], accroître considérablement leur application pour de nombreuses applications liées à la détection, estimation, prédiction, reconnaissance, classification, etc.

L'objectif de ce projet de thèse est d'apporter une contribution dans ce domaine en exploitant les modèles de Transformers et de proposer de nouveaux algorithmes de détection des troubles dépressifs à partir des signaux EEG.

En termes d'application, ce projet vise à apporter des solutions d'intelligence artificielle innovantes dans le domaine de la santé mentale, en particulier, assister le staff médical dans les hôpitaux au diagnostic des troubles dépressifs nécessitant une hospitalisation.

Références :

- [1] J. Zhu et al., "EEG-based depression recognition using improved graph convolutional neural network", Computers in Biology and Medicine, vol. 148, 105815, 2022.
- [2] A. Dev et al., "Exploration of EEG-Based Depression Biomarkers Identification Techniques and Their Applications: A Systematic Review", IEEE Access, vol. 10, pp. 16756-16781, 2022.
- [3] K. Han et al., "A Survey on Vision Transformer", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 45, no. 1, pp. 87-110, 2023.

Annexe n°4 : Plan de recherche 9

Approche guidée par la qualité de données pour une gestion automatique des systèmes de systèmes cyber-physiques dynamiques

✓ Contexte de recherche :

Ces dernières années, nous avons assisté à la convergence des systèmes Informatiques vers des écosystèmes complexes connus sous le nom de systèmes de systèmes cyber-physiques (SSCP) induits par les progrès technologiques, notamment l'Internet des objets (IdO). Les SSCP jouent un rôle crucial dans une multitude de domaines, tels que la santé, les transports, l'industrie et le développement des villes intelligentes. Un exemple concret illustrant cette évolution est celui des jumeaux numériques. Ces derniers représentent des répliques virtuelles de systèmes physiques, permettant de modéliser, de superviser, d'analyser, et de gérer un système physique. Ce genre de systèmes intègrent des données en temps réel provenant des systèmes physiques et virtuels, des données historiques, et des informations contextuelles plus riches et plus complexes, nécessitant une synchronisation bidirectionnelle.

Dans ce cadre, la qualité des données revêt une importance capitale. En effet, des données erronées ou incomplètes peuvent conduire à des décisions automatisées non optimales, voire entraîner des conséquences indésirables, pouvant compromettre l'efficacité et la fiabilité du système. La précision et l'intégrité des données sont donc des éléments essentiels pour garantir la pertinence et la fiabilité des analyses effectuées, et par extension, pour assurer le bon fonctionnement et la fiabilité du système dans son ensemble.

Cette thèse se focalise sur l'exploration de la gestion automatisée des SSCP en mettant particulièrement l'accent sur l'importance cruciale de la qualité des données. Les étapes visées sont comme suit :

- Étude de l'état de l'art sur la qualité des données, les SSCP, et leur gestion,
- Proposition d'un scénario applicatif dans le domaine des jumeaux numériques
- Élaborer des méthodes et des techniques d'analyse et de validation des données
- Proposition d'une approche de gestion automatique des CSP qui tienne compte de la qualité des données
- Implémentation et évaluation des solutions proposées
- Publication et présentation des résultats dans des conférences de renommée internationale

✓ Résumé et mots clés :

mots IoT, systèmes cyber-physiques, systèmes de systèmes cyber-physiques, qualité des données, précision des données, intégrité des données, jumeaux numériques, apprentissage automatique, apprentissage profond

Annexe n°4 : Plan de recherche 10

Privacy-preserving data analytics at scale - Application to Healthcare

✓ Contexte de recherche :

Ceic rentre dans le cadre de la recherche dans le domaine de Big Data pour la santé public.

✓ Résumé et mots clés :

Most of the data collected in recent years is private or has elements of sensitivity that need to be protected. Many data analytics studies have been conducted on those large datasets without paying attention to the privacy element of the data at hand. However, this must change, and it is not ethical to gather the data with sensitive information without guaranteeing the privacy of individuals and institutions. Collecting and analysing data at a large scale offer significant value for individuals and businesses. Furthermore, this can significantly affect society through increased productivity, reduced garbage, and saved time. However, existing technologies and regulations cannot support a privacy-guaranteed data management lifecycle. The main objective of this project is to develop novel efficient privacy-preserving techniques that scale across Big Data analysis technologies while adapting to undefined dataset sizes, variety, and velocity. The proposed solutions will be tested and validated on healthcare systems, which are critical to our society and economy.

Annexe n°4 : Plan de recherche 11

Real-Time anomaly detection framework for cyberattacks targeting sensor data in Cyber-Physical Systems.

✓ Contexte de recherche :

The increasing reliance on Cyber-Physical Systems (CPS) in critical infrastructure, like power grids and water treatment plants, creates vulnerabilities to cyberattacks that manipulate sensor data. These attacks can disrupt critical operations, leading to cascading failures with disastrous consequences. Existing IT security measures are insufficient as they don't monitor the physical layer or effectively defend against sophisticated attacks.

This project aims to develop a real-time anomaly detection framework. The successful development of this framework can significantly enhance the security of critical infrastructure by proactively detecting cyberattacks before they disrupt essential services. This can have a positive impact on national security, public safety, and economic stability.

✓ Résumé et mots clés :

This project addresses a critical need for robust cybersecurity solutions in critical infrastructure Cyber-Physical Systems (CPS). The growing reliance of critical infrastructure, such as oil refining, power grids and water treatment plants, introduces new security challenges. CPS integrate physical processes with computer control, making them vulnerable to complex cyberattacks. These attacks manipulate sensor data, leading to disruptions in critical operations. By developing a real-time anomaly detection framework, this research aims to improve the resilience of these systems and safeguard essential services from cyberattacks. The project's findings can benefit both academic researchers and industry professionals working on securing CPS and critical infrastructure.

Mots clés : Cyber-Physical Systems, anomaly detection framework, cyberattacks.

Annexe n°4 : Plan de recherche 12

Méthodes d'Intelligence Artificielle pour l'Internet du comportement

✓ Contexte de recherche :

Ce projet de thèse se situe dans le domaine de l'Internet des comportements (IoB pour Internet of Behaviors) où l'objectif est d'analyser des données liées aux tendances comportementales des utilisateurs pour réaliser un objectif particulier. Ces données sont collectées par des dispositifs intelligents et reflètent le comportement, les habitudes et le mode de vie des utilisateurs dans différents domaines tels que la santé, le transport, l'éducation, l'énergie, etc. En développant des méthodes avancées de collecte et d'analyse de données, cette thèse vise à repousser les limites de la recherche sur l'IoB et à ouvrir de nouvelles perspectives dans le domaine du ciblage comportemental. Les travaux de recherche réalisés dans le cadre de cette thèse visent à développer des techniques novatrices de ciblage comportemental en s'appuyant sur des méthodes d'analyse avancée telles que le Machine Learning et le Deep Learning.

✓ Résumé et mots clés :

Cette thèse offre des possibilités prometteuses pour améliorer l'efficacité des stratégies de ciblage dans le domaine de l'éducation. En fournissant des données sur les comportements individuels et collectifs des individus, cette recherche peut aider les étudiants et les enseignants (ou les apprenants et les formateurs de manière générale) à améliorer leurs expériences d'apprentissage et performances académiques. Par exemple, en analysant le comportement des étudiants en classe, les institutions éducatives peuvent mieux comprendre les schémas d'apprentissage et adapter leurs méthodes d'enseignement afin de répondre aux besoins individuels des étudiants. Les enseignants peuvent également identifier les signes de décrochage ou des besoins spécifiques en matière de soutien, leur permettant d'intervenir de manière proactive pour offrir des mécanismes permettant d'améliorer les résultats académiques globaux. De plus, en explorant les implications éthiques et sociales de l'utilisation de l'IoB dans le ciblage comportemental, cette thèse contribuera à façonner les discussions sur la protection de la vie privée, la transparence des données et la responsabilité sociale des organisations.

Mots-clés: Intelligence Artificielle, Analyse comportementale, éducation

Annexe n°4 : Plan de recherche 13

Neuro-Symbolic Approaches for Advanced Biological Data Management and Analysis

✓ Contexte de recherche :

The increasing digitization of healthcare and biological research has catalysed an unprecedented influx of data, comprising various biological test results such as medical lab reports, genetic sequences, proteomics, and metabolomics data. This vast reservoir of information harbours immense potential for pioneering breakthroughs in health sciences, fostering advancements in personalised medicine, and shaping innovative treatment strategies.

Yet, harnessing the full potential of these datasets poses formidable challenges, primarily stemming from inherent data quality issues. Biological test results are frequently beset by uncertainties, ranging from measurement errors and missing values to temporal and source-based variabilities. Moreover, discrepancies arising from disparate measurement techniques and instruments further compound the complexity, impeding direct comparisons and comprehensive analyses.

Conventional database management systems, characterised by their reliance on exact matches and deterministic equality conditions, prove inadequate for handling the intricacies of biological datasets. In the realm of biology, interpretations of equality often extend beyond binary notions, encompassing diverse degrees of similarity and functional relationships between data points. Addressing these nuanced interpretations necessitates the adoption of sophisticated data management techniques transcending conventional methodologies.

To confront these challenges head-on, this thesis embarks on a journey to explore advanced methodologies for managing biological data. By leveraging a neuro-symbolic framework, integrating neural network-based learning with symbolic reasoning, this research endeavours to unravel the complexities inherent in biological test results. Through the application of neuro-symbolic approaches, including lattice-based declarative frameworks and embeddings, this study seeks to furnish a more nuanced representation of biological data. By accommodating diverse contexts and elucidating intricate functional dependencies, these methodologies aim to facilitate precise data selection and efficient retrieval, thus poised to revolutionise data-driven insights in biological research and healthcare.

✓ Résumé et mots clés :

In this PhD thesis, we delve into the innovative realm of neuro-symbolic methodologies, integrating a lattice-based declarative framework, comparability functions, and embeddings to revolutionize the management of biological test results. Our overarching objective is to sculpt a holistic approach that encapsulates the multifaceted nature of biological data, surmounting the inherent complexities and uncertainties pervading the domain.

The research unfolds across the following pivotal components:

1. **Lattice-Based Framework with Neuro-Symbolic Integration:** We pioneer the development of a cutting-edge framework melding neural network-based learning with symbolic reasoning within a lattice-based structure. This amalgamation empowers nuanced interpretations of equality and fosters context-dependent comparisons, thereby enriching the management of biological test results.
2. **Neuro-Symbolic Embeddings for Enhanced Representation:** We embark on the creation of neuro-symbolic embeddings, orchestrating the transformation of biological data into a continuous, lower-dimensional space. These embeddings transcend traditional representations, facilitating more effective navigation through uncertainty, missing values, and semantic similarities inherent in biological datasets.
3. **Exploration of Neuro-Symbolic Functional Dependencies:** We embark on a deep dive into abstract functional dependencies within the neuro-symbolic paradigm, unravelling intricate relationships between diverse biological attributes. This exploration unveils the underlying dynamics governing data selection and querying, paving the way for enhanced analytical capabilities.
4. **Applications and Evaluations in Real-World Biological Contexts:** We embark on a transformative journey, applying our neuro-symbolic methodologies to real-world biological datasets, including medical test results. Through rigorous evaluation, we elucidate the tangible benefits of our approach, spanning improved data selection, refined predictive modelling, enhanced anomaly detection, and ultimately, augmented patient outcomes.

In sum, this thesis constitutes a pioneering contribution to the realm of data management, transcending conventional boundaries through the infusion of neuro-symbolic methodologies. By equipping researchers and practitioners with advanced techniques tailored to the idiosyncrasies of biological data, our work holds the promise of ushering in a new era of precision and reliability in data-driven insights across the biological and medical domains.

Keywords: Neuro-Symbolic, Biological Data, Data Management, Lattice-Based Framework, Embeddings, Functional Dependencies, Data Quality, Uncertainty, Healthcare Informatics.

Annexe n°4 : Plan de recherche 14

Network Intrusion Detection

✓ Contexte de recherche :

Most nowadays computer systems are connected to a network, whether Internet or a smaller scale network. This has made network connections one of the main attack delivery mechanisms. Security-aware organisations monitor their traffic to detect traces of attacks on, and from, their infrastructure. The amount of traffic data generated per second is too large to be manually checked and cybersecurity firms propose a wide range of network monitoring tools that aggregate data and use pre-defined rules and signatures to detect attacks. These techniques are quite rigid and are easy to evade by zero-day attacks and by varying the attack patterns (by, say, adding extra useless messages that change the attack's signature).

Machine-learning-based methods are resilient to minor variations in attack patterns, and are of generalising enough to be able to detect new attacks.

In this research, we will propose machine-learning-based methods for network intrusion detection.

✓ Résumé et mots clés :

We aim to devise modern machine learning-based methods for network intrusion detection. Potential approaches we would explore for that purpose could include, but are not limited to:

- Natural Language Processing: by looking at the network traffic as a conversation.
- Active, aka Online, learning: to continuously update the network attack detector.

The final decision of which approaches we will explore will be made based on the literature review.

Candidates are invited to directly contact me on h.ragabhassen@hw.ac.uk should they wish to have a conversation about the topic before selecting it.

Recommended reading:

- <https://nostarch.com/packetanalysis3>
- <https://www.sciencedirect.com/science/article/abs/pii/S1084804520302411>
- https://link.springer.com/chapter/10.1007/978-3-031-40598-3_3

Keywords

Network intrusion detection, active learning, machine learning, natural language processing, deep learning.

Annexe n°4 : Plan de recherche 16

Analyse Multi-Omique Intégrative pour la Prédiction des Interactions Protéine-Protéine dans la Découverte de Médicaments : Vers des Interventions Thérapeutiques Ciblées

✓ Contexte de recherche :

✓ Résumé et mots clés :

Les interactions protéine-protéine (IPP) jouent un rôle essentiel dans les voies de signalisation cellulaires et représentent des cibles prometteuses pour la découverte de médicaments. L'intégration de données multi-omiques, comprenant la génomique, la transcriptomique, la protéomique et la métabolomique, offre une approche complète pour élucider les interactions moléculaires complexes sous-jacentes aux mécanismes des maladies et identifier les complexes protéiques pouvant être ciblés par des médicaments. Dans cette étude, nous proposons un cadre d'analyse multi-omique intégrative pour prédire les IPP afin d'accélérer les pipelines de découverte de médicaments. En exploitant des données omiques de haute dimension, telles que les profils d'expression génique, les niveaux d'abondance des protéines et les modifications post-traductionnelles, nous utilisons des méthodes statistiques et des algorithmes avancés d'apprentissage automatique pour inférer les réseaux d'interaction protéique et prioriser les cibles potentielles de médicaments.

Mots clés: IPP, voies de signalisation cellulaires, protéines cibles, découverte de médicaments, analyse multi-omique intégrative, Apprentissage automatique.

Annexe n°4 : Plan de recherche 17

Multi-source Data Integration for Enhanced Flood Prediction

✓ **Contexte de recherche :**

✓ **Résumé et mots clés :**

This project aims to improve flood prediction accuracy by integrating diverse data sources, such as meteorological data, hydrological models, satellite imagery, and social media feeds. The main objectives include developing robust algorithms for data fusion, creating predictive models that leverage integrated data, and validating these models against historical flood events. The ultimate goal is to provide more reliable and timely flood forecasts to aid in disaster preparedness and response.

Annexe n°4 : Plan de recherche 18

Cybersécurité des données médicales des patients à base des STaaS-Cloud.

✓ Contexte de recherche :

Le contexte de recherche de ce sujet s'intègre dans le domaine de la santé des citoyens est plus particulièrement les données médicales d'un patient et sa santé. L'utilisation des services du Cloud dans ce domaine a vu une grande croissance. Cette utilisation permet de mieux gérer ces données telles que les symptômes d'une maladie, d'obtenir des diagnostics pertinents, d'identifier les facteurs de risque, de détecter et de prédire les maladies.

✓ Résumé et mots clés :

Annexe n°4 : Plan de recherche 19

Advancing Radiology Reporting through Collaborative AI-Enabled Approaches

✓ Contexte de recherche :

The research context in radiology report generation is marked by a growing need for accurate, timely reports amid increasing volumes of imaging data. Integrating artificial intelligence (AI) presents opportunities for improving efficiency and diagnostic accuracy. Current research focuses on developing AI-enabled solutions to streamline reporting workflows, enhance diagnostic capabilities, and address challenges such as interpretability, workflow integration, and ethical considerations. The goal is to leverage AI to augment radiologists' capabilities and improve patient outcomes in radiology practice

✓ Résumé et mots clés :

The advent of artificial intelligence (AI) has revolutionized radiology reporting, offering unprecedented opportunities for efficiency, accuracy, and innovation. However, to fully harness the potential of AI in radiology reporting, it is essential to explore novel approaches that combine AI capabilities with human expertise. This paper proposes a comprehensive framework for advancing radiology reporting through collaborative AI-enabled approaches. We outline six key strategies, including Explainable AI (XAI), AI-assisted report writing, collaborative learning, leveraging multimodal data, integration with Radiology Information Systems (RIS) and Electronic Medical Records (EMR), and standardization of reports. These approaches not only enhance the quality and efficiency of radiology reporting but also promote synergistic interactions between AI systems and radiologists. We discuss the potential benefits, challenges, and future directions of each approach and highlight their implications for clinical practice and research. By embracing collaborative AI-enabled approaches, we can unlock new frontiers in radiology reporting, ultimately improving patient care and outcomes. Keywords: Radiology reporting, Artificial Intelligence, Explainable AI, Collaborative learning, Multimodal data, Radiology Information Systems, Electronic Medical Records, Standardization.

Annexe n°4 : Plan de recherche 21

Amélioration de la détection d'anomalies dans les séquences vidéo pour la sécurité énergétique

✓ Contexte de recherche :

La surveillance efficace des installations énergétiques est cruciale pour prévenir les interruptions de service et garantir une fourniture énergétique stable. L'utilisation des séquences vidéo, couplée aux progrès de l'analyse d'image et de l'apprentissage automatique, représente une solution prometteuse pour identifier rapidement et précisément les comportements anormaux ou les défauts techniques. Les défis principaux résident dans le traitement de ces données vidéo volumineuses, générées en continu, afin de détecter les anomalies en temps réel. Cela nécessite une gestion sophistiquée des ressources computationnelles pour le traitement parallèle et distribué, et des techniques qui doivent être robustes, évolutives, et capables de fonctionner dans des conditions critiques de réactivité [Zhang et al., 2019].

✓ Résumé et mots clés :

1. Défis scientifiques

- Analyse de données en haute dimension : Développement de méthodes pour gérer et analyser efficacement des flux vidéo en haute résolution pour la détection rapide des anomalies, en utilisant des techniques d'apprentissage profond et d'analyse de séries temporelles adaptées aux caractéristiques visuelles et temporelles des vidéos [Feng et al., 2018 ; Benkabou et al. 2018 ; Benkabou et al. 2022].
- Traitement parallèle et distribué : Conception d'architectures logicielles qui facilitent la distribution et la parallélisation des tâches de calcul afin de traiter efficacement les données sur des infrastructures de cloud computing ou des systèmes de calcul haute performance [Sharma et al., 2021].
- Intégration de capteurs et de données multimodales : Exploitation des données issues de divers capteurs (thermiques, acoustiques, etc.) en combinaison avec les séquences vidéo pour améliorer la précision de la détection des anomalies [Zhang et al., 2022].
- Robustesse et adaptation en temps réel : Assurer la capacité du système à s'adapter aux changements de conditions environnementales et opérationnelles sans diminution de la performance [Sun et al., 2023].

2. Objectifs

- Développement d'un modèle de détection d'anomalies : Création d'un modèle robuste utilisant l'apprentissage profond pour identifier les anomalies dans les vidéos de surveillance des infrastructures énergétiques [Lee et al. 2023; Lu et al. 2023; Mohammad et al. 2023].
- Optimisation des performances en temps réel : Amélioration de la vitesse et de la précision des prédictions en optimisant les algorithmes pour le traitement parallèle [Chen et al., 2019].
- Validation empirique : Test et validation du modèle sur des ensembles de données réels, en simulant des scénarios d'anomalies typiques et atypiques pour évaluer la performance du système [Wenig al., 2022].
- Contribution à la sécurité énergétique : Démonstration de comment une surveillance vidéo avancée peut contribuer significativement à la sécurité et à l'efficacité des infrastructures énergétiques [Reddicharla et al., 2020].

Références

1. Zhang, Q., Sun, H., Wu, X., & Zhong, H. (2019). Edge video analytics for public safety: A review. *Proceedings of the IEEE*, 107(8), 1675-1696.
2. Feng, Weita, et al. "Challenges on large scale surveillance video analysis." *Proceedings of the IEEE conference on computer vision and pattern recognition workshops*. 2018.
3. Seif-Eddine Benkabou, Khalid Benabdeslem, Vivien Kraus, Kilian Bourhis, Bruno Canitia. Local Anomaly Detection for Multivariate Time Series by Temporal Dependency Based on Poisson Model. *IEEE Trans. Neural Networks Learn. Syst.* 33(11): 6701-6711 (2022)
4. Seif-Eddine Benkabou, Khalid Benabdeslem, Bruno Caniti. Unsupervised outlier detection for time series by entropy and dynamic time warping. *Knowl. Inf. Syst.* 54(2): 463-486 (2018)
5. Sharma, Vijeta, et al. "Video processing using deep learning techniques: A systematic literature review." *IEEE Access* 9 (2021): 139489-139507.
6. Zhang, Chaobo, et al. "A real-time abnormal operation pattern detection method for building energy systems based on association rule bases." *Building Simulation*. Vol. 15. No. 1. Beijing: Tsinghua University Press, 2022.
7. Sun, Xudong, et al. "Survey of distributed computing frameworks for supporting big data analysis." *Big Data Mining and Analytics* 6.2 (2023): 154-169.
8. Lee, Sangkeum, et al. "Anomaly detection of smart metering system for power management with battery storage system/electric vehicle." *ETRI Journal* 45.4 (2023): 650-665.
9. Lu, Tianyuan, Lei Wang, and Xiaoyong Zhao. "Review of anomaly detection algorithms for data streams." *Applied Sciences* 13.10 (2023): 6353.
10. Mohammad, Ashif, and Farhana Mahjabeen. "Revolutionizing solar energy with ai-driven enhancements in photovoltaic technology." *BULLET: Jurnal Multidisiplin Ilmu* 2.4 (2023): 1174-1187.
11. Chen, Jianguo, et al. "Distributed deep learning model for intelligent video surveillance systems with edge computing." *IEEE Transactions on Industrial Informatics* (2019).
12. Wenig, Phillip, Sebastian Schmidl, and Thorsten Papenbrock. "TimeEval: A benchmarking toolkit for time series anomaly detection algorithms." *Proceedings of the VLDB Endowment* 15.12 (2022): 3678-3681.

Annexe n°4 : Plan de recherche 22

Sécurité dans l'Internet des comportements (IoB)

✓ Contexte de recherche :

Confidentialité des données : Protéger les informations comportementales contre l'accès non autorisé et garantir leur confidentialité.

Intégrité des données : Assurer l'exactitude et la fiabilité des données collectées et analysées.

Authentification et Autorisation : Mettre en place des mécanismes robustes pour vérifier les identités et contrôler les accès.

Gestion des identités et des accès (IAM) : Développer des systèmes efficaces pour gérer les identités et sécuriser les accès.

Protection de la vie privée : Intégrer des techniques pour protéger les données personnelles et respecter la vie privée des utilisateurs.

Sécurité des communications : Assurer des échanges de données sécurisés entre les dispositifs IoB et les systèmes centraux.

Résilience et fiabilité des systèmes : Concevoir des systèmes capables de résister aux attaques et de maintenir leur fonctionnement en toutes circonstances.

✓ Résumé et mots clés :

L'Internet des Comportements (IoB) représente une avancée technologique majeure qui permet de collecter, analyser et utiliser les données comportementales pour influencer les actions des individus. Bien que l'IoB offre des avantages considérables dans divers domaines tels que le marketing, la sécurité publique, et la gestion des ressources humaines, il soulève également des préoccupations critiques en matière de sécurité et de confidentialité des données. Cette thèse propose d'explorer les enjeux de sécurité liés à l'IoB, d'identifier les défis principaux et de développer des solutions innovantes pour protéger les données et assurer un usage éthique de cette technologie.

Annexe n°4 : Plan de recherche 23

LLMs at the rescue of fake news -- Case study to journalism

✓ Contexte de recherche :

Build expertise in LLM technology and contribute to its use to real-world data-driven applications

✓ Résumé et mots clés :

The rapid development of Large Language Models (LLMs) like GPT-4, Claude-3, and Gemini has transformed the field of natural language processing. However, it has also resulted in a significant issue known as Benchmark Data Contamination (BDC). This occurs when language models inadvertently incorporate evaluation benchmark information from their training data, leading to inaccurate or unreliable performance during the evaluation phase of the process.

First, one should review the complex challenge of BDC in LLM evaluation and explores alternative assessment methods to mitigate the risks associated with traditional benchmarks. The next step is to examines challenges and future directions in mitigating BDC risks, highlighting the complexity of the issue and the need for innovative solutions to ensure the reliability of LLM evaluation in real-world applications. Finally, propose innovative solutions to build appropriate LLM and train it on real-world datasets.

Annexe n°4 : Plan de recherche 24

Reinforcement learning for optimization of vehicle platooning on highways.

✓ Contexte de recherche :

As autonomous driving technology advances, automated platooning is increasingly being explored as a promising solution to improve traffic flow in transportation networks. Platoon-based driving involves a cooperative driving pattern in which a group of vehicles moves at a consensual speed while maintaining a small, nearly constant distance between adjacent vehicles. A well-developed platooning system can significantly enhance safety performance by employing stable automation control [1]. Additionally, shorter following distances can reduce air resistance, improving fuel efficiency and reducing exhaust emissions,

particularly for trucks. Traffic flow optimization is a primary motivation for developing platoon-based driving models and algorithms, as exemplified by the California Partners for Advanced Transit and Highways (PATH) project [2]. Compared to independent vehicles, platoons require less road space and can improve road capacity, resulting in reduced congestion and smoother traffic flow without the need for constructing new facilities. To achieve platoon stability, four key components are generally considered [3]: 1) node dynamics (ND), which describes the behavior of each platoon member; 2) information flow topology (IFT), which defines how information is exchanged between vehicles; 3) distributed controller (DC), which provides feedback control of the platoon; and 4) geometry formation (GF), which establishes the expected inter-vehicle distance. Extensive research has been conducted on optimizing platoon-based driving. For many years, reinforcement learning (RL) algorithms have been proposed for cruise control, which is a crucial component of vehicle platooning. In [6], RL was employed for cooperative adaptive cruise control, utilizing gradient-descent learning algorithms, while in [7], the authors addressed adaptive cruise control issues by utilizing supervised actor-critic RL for acceleration controllers, with lower-level control managed by throttle and brake controllers. In [8], three model-free RL algorithms and one model-based algorithm were used to maintain the vehicle within its lanes at the desired speed. More recently, the authors of [9] proposed an RL-based

approach for multi-vehicle platooning using an optimal gap controller, based on an actor-critic RL policy with a deep deterministic policy gradient algorithm.

At the Cosys/Grettia laboratory, we work on the optimization of traffic in transportation networks, utilizing various approaches such as discrete optimization, multi-criteria optimization, optimal control, dynamic programming, among others. In recent years, we have been exploring the use of reinforcement learning, an artificial intelligence approach that has shown remarkable effectiveness in several areas. Accordingly, we have developed reinforcement learning models and algorithms to understand and optimize the lane-changing process on highways [10], and to optimize the management of mixed urban traffic through traffic lights [11]. Additionally, we have initiated efforts to optimize platoon-based driving in mixed traffic [12].

✓ Résumé et mots clés :

Reinforcement learning , optimization , vehicle platooning , transportation.

Annexe n°4 : Plan de recherche 25

Apprentissage multi-vue pour la détection d'anomalies cardiaques à partir de données multi-sources

✓ Contexte de recherche :

Les observations cliniques en cardiologie ont montré que les cardiomyopathies héréditaires sont des maladies graves, complexes et mal comprises qui affectent des millions de jeunes patients à travers le monde, notamment dans les terrains de sport, pouvant provoquer la mort subite. Plus d'un millier de mutations ont été identifiées dans de nombreux gènes, indiquant que diverses molécules et voies entraînent des cardiomyopathies hypertrophiques, dilatées, restrictives et arythmogènes. Ces mutations sont souvent spécifiques à un patient, pertinentes pour une personne, ou spécifiques à un groupe, c'est-à-dire caractéristiques de populations de patients sous-spécifiques. Cependant, l'hétérogénéité génétique et la variation allélique associées à la variation de l'expression clinique posent des défis importants aux cliniciens face à un individu. De plus, le phénotypage faible limite la puissance de l'analyse génétique.

Les données récoltées sur les patients, aussi bien cliniques que biologiques, représentent un important centre d'intérêt et de préoccupation pour les professionnels de la santé. Elles constituent en effet, un gisement considérable de signaux cardiaques (ECG) et de variantes génétiques, en guise d'un phénotypage clinique pertinent sur la maladie, obtenu grâce à un profiling clinico-biologique précis pour les professionnels de la santé. Il est donc primordial pour ces derniers de disposer d'un tableau de « bord » efficace permettant d'une part, de diagnostiquer au mieux la cardiomyopathie héréditaire et d'autre part, de servir comme outil d'aide à la décision thérapeutique. Actuellement, Le diagnostic de la cardiomyopathie chez un patient donné est simple et incomplet et sera certainement amélioré en combinant des données cliniques et de génotypage. À leur tour, les profils clinico-biologiques obtenus, établis comme des empreintes, aideront à adapter la thérapie à différents patients ou groupes de patients. Cependant, l'obtention de tels profils nécessiteront un traitement automatisé et optimal face à la quantité massive de données médicales disponibles.

✓ Résumé et mots clés :

Le diagnostic automatique à partir de données mixtes est une tâche immense, sachant qu'il existe actuellement environ un volume considérable d'enregistrements ECG et de signatures génétiques dans le référentiel des hôpitaux, non structurés en provenance de sources hétérogènes.

De manière synoptique, l'objectif final de notre recherche est d'automatiser la création et l'enrichissement des bases de données contenant les caractéristiques et les comportements cardiaques et héréditaires, en vue d'un diagnostic optimal des pathologies sous-jacentes.

Étant donnée la nature complexe des données récoltées sur les patients, un des besoins exprimés par les professionnels de la santé couvrent les aspects suivants, qui constituent les objectifs opérationnels et scientifiques du projet :

- Besoin en détection d'anomalies : Il s'agit de détecter des signaux ECG globalement déviants ou les séquences temporelles qui posent problème afin de mettre en avant les impulsions électriques aberrantes. Ce niveau de détection est intéressant pour écarter les données « suspectes » qui pourraient drastiquement biaiser le profiling des patients. Cette suspicion sur les données peut avoir lieu aussi bien sur la partie des signaux cardiaques que sur la partie biologique à fortes mutations génétiques.

Annexe n°4 : Plan de recherche 26

Mise en place d'un jumeau numérique pour améliorer l'apprentissage des drones dans le suivi d'objets en vol

✓ Contexte de recherche :

L'objectif est d'explorer l'intégration de la technologie des jumeaux numériques pour améliorer le processus d'apprentissage des tâches de suivi d'objets basées sur des drones. La technologie des jumeaux numériques crée une réplique virtuelle d'actifs ou de systèmes physiques, permettant une surveillance, une analyse et une simulation en temps réel. Cette recherche se concentre sur l'utilisation des jumeaux numériques pour améliorer la formation et la performance des drones dans le suivi d'objets en mouvement pendant le vol. En développant un modèle de jumeau numérique qui reflète l'environnement physique et les dynamiques rencontrés par les drones, la thèse cherche à fournir une plateforme de formation réaliste et adaptable. À travers des expérimentations approfondies et des validations, la recherche évaluera l'efficacité de l'utilisation des jumeaux numériques pour améliorer les algorithmes d'apprentissage des drones pour les tâches de suivi d'objets. De plus, la thèse examinera la scalabilité et la transférabilité du cadre de jumeau numérique développé sur différentes plates-formes de drones et dans des scénarios opérationnels variés. En comblant le fossé entre les environnements virtuels et physiques, cette recherche vise à faire progresser les capacités des drones dans diverses applications, notamment la surveillance, la recherche et le sauvetage, et la navigation autonome. La mise en œuvre du jumeau numérique sera validée par des tests rigoureux et des simulations, garantissant son efficacité et son applicabilité dans les opérations réelles des drones. Grâce à cette approche interdisciplinaire, la thèse vise à contribuer à l'avancement de la technologie des drones et à son intégration dans divers domaines.

✓ Résumé et mots clés :

Cette thèse vise à explorer l'utilisation de la technologie des jumeaux numériques, qui créent des répliques virtuelles d'environnements physiques, pour améliorer l'apprentissage et les performances des drones dans le suivi d'objets en mouvement. L'objectif est de développer un modèle de jumeau numérique simulant les conditions réelles rencontrées par les drones, afin de fournir une plateforme de formation réaliste et adaptable. La recherche évaluera l'efficacité de cette approche pour optimiser les algorithmes d'apprentissage des drones, tout en examinant la scalabilité et la transférabilité du cadre développé sur différentes plates-formes. En comblant le fossé entre les environnements virtuels et physiques, cette thèse vise à faire progresser les capacités des drones dans diverses applications, telles que la surveillance, la recherche et le sauvetage, et la navigation autonome.

Mots clés:

Jumeaux numériques

Drones

Suivi d'objets

Apprentissage par simulation

Environnements virtuels

Réalité augmentée

Vision par ordinateur

Réseaux de neurones

Apprentissage en profondeur

Annexe n°4 : Plan de recherché 27

Intelligent models for Privacy and trust in Internet of Things ecosystems

✓ Contexte de recherche :

The objective is to develop new techniques and models to address the privacy and trust challenges in Internet of Things (IoT)-based smart systems.

✓ Résumé et mots clés :

The Internet of Things (IoT) is transforming many leading industries. IoT deployments involve the use of diverse devices with computing and communication capabilities that need to work together to perform specific and complex tasks. The data collected, exchanged, analysed and transformed within IoT systems or on remote infrastructures is used to make decisions that improve productivity and efficiency in major industries such as energy, agriculture, transportation and healthcare. In this context, it is important to ensure privacy, security of shared data and system reliability.

In IoT systems, the concept of privacy has been extensively explored in the academic literature. Similarly, trust and trustworthy behaviour have been studied extensively. However, there is a lack of work that investigates both privacy and trust simultaneously. Harmonising privacy, trust and trustworthiness will facilitate the widespread adoption of IoT technologies while considering energy, delay and computation ressources constraints.

The aim of this thesis is to understand the interrelationship between privacy, trust and trustworthiness in the IoT domain, and then to develop new techniques and models to address these open issues in (IoT)-based smart systems. Potential applications include energy, agriculture, transportation and healthcare.

key words: IoT, security, optimization

Annexe n°4 : Plan de recherche 28

Adaptive Defense Strategies Using LLMs: Developing Context-Aware Security Protocols for Dynamic Threat Landscapes

✓ **Contexte de recherche :**

✓ **Résumé et mots clés :**

The rapidly evolving landscape of cybersecurity threats necessitates the development of robust and flexible defense mechanisms. This doctoral project focuses on leveraging the capabilities of Large Language Models (LLMs) to develop adaptive defense strategies that are sensitive to the context and dynamics of emerging threats. The core objective is to innovate context-aware security protocols that dynamically adjust to fluctuating threat environments, significantly enhancing the resilience and responsiveness of cybersecurity systems. By integrating the predictive power and contextual understanding of LLMs, this research aims to anticipate and counteract novel attack vectors promptly. Through systematic development and rigorous testing, the project seeks to establish a new paradigm in cybersecurity that underscores adaptability and proactive defense, potentially setting a benchmark for future security frameworks in various technological arenas.

Annexe 5 : Fiche de synthèse

ملحق بالقرار رقم المؤرخ في
والمتضمن تأهيل المدرسة العليا في علوم وتكنولوجيات الإعلام الآلي و الرقمنة لضمان التكوين لنيل شهادة الدكتوراه
ويحدّد عدد المناصب المفتوحة بعنوان السنة الجامعية 2025-2024

Domaine	Filière	Responsable de la filière (Formation doctorale)	Spécialités	Nombre de places pédagogiques par spécialité	Total (Filière)
MI	Informatique	SEBAA Abderrazak	Intelligence Artificielle	18	28
			Réseaux & Sécurité	10	

Annexe 6 : Avis et Visas des organes administratifs et scientifiques

Signature du responsable de la formation doctorale :

Dr. SEBAI Abdelrazak

CSF (faculté) ou CSI (institut) ou CSD (Ecole)

Avis et visa:

Favorable

Date : 30 MAI 2024

رئيس المجلس العلمي
الأستاذ: طاري عبد الكمال



Conseil du laboratoire ou autres structures

Avis et visa:

Favorable
Pr. DIENABET Ali
Laboratoire d'Informatique et des Technologies Avancées de Numériques -LITAN-

Date : 30 MAI 2024

Pr SLIMANI Hachem

الأستاذ سليماني هاشم

Favorable
Laboratoire d'Informatique Médicale
مختبر المعلوماتية

Chef d'établissement

Avis et visa du Chef d'établissement:

Favorable

Date : 30 MAI 2024

مدير المدرسة العليا في العلوم والتكنولوجيا
الإعلام الآلي والرقمنة
الأستاذ: طاري عبد الكمال

