2025, vol. 5, n° 1, 121-145 pages, DOI : 10.21494/ISTE.OP.2025.1302 ISTE OpenScience

INFORSID 2024 Forum Jeunes Chercheuses Jeunes Chercheurs

INFORSID 2024 Forum of junior researchers

Mario Cortes Cornax[1], Marin Francois[2], Qinyue Liu[1], Ibrahim Mohamed Serouis[3], Vlada Stegarescu[4]

[1] Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG, 38000 Grenoble, France 150 Pl. du Torrent, 38400Saint-Martin-d'Hères, France, prenom.NOM@univ-grenoble-alpes.fr
[2] Université Paris-Dauphine, PSL, LAMSADE UMR CNRS 7243, DRM UMR CNRS 7088, Place du Maréchal de Lattre deTassigny, 75775 Paris, France, marin.francois@dauphine.psl.eu
[3] Université Paul Sabatier, Laboratoire IRIT, 118 Route de Narbonne, 31062, Toulouse,ibrahim.mohamed-serouis@irit.fr
[4] IRIT, CNRS (UMR 5505), Université Toulouse Capitole, Akkodis Toulouse, France, vlada.stegarescu@(irit.fr, akkodis.com)

RÉSUMÉ. Cet article présente une sélection de quatre des treize articles courts du Forum Jeunes Chercheuses Jeunes Chercheurs (JCJC) d'INFORSID 2024. Il offre un panorama de la recherche française menée par des doctorants en systèmes d'information. Ces travaux témoignent de l'engagement de la communauté à développer des systèmes responsables, tant sur le plan sociétal qu'environnemental. Certains explorent également les nouvelles innovations en intelligence artificielle. Cet article aborde divers thèmes tels que la sécurité, l'intégrité de la recherche, l'analyse multimodale de scènes et la frugalité des données.

ABSTRACT. This article presents a selection of four of the thirteen short papers from the Forum for Young Researchers (JCJC) at INFORSID 2024. It provides a snapshot of the French research landscape as seen by PhD students in information systems. These works demonstrate the community's commitment to developing responsible systems, both socially and environmentally. Some of the studies also consider new innovations in artificial intelligence. This article covers various themes such as security, research integrity, multimodal scene analysis, and data frugality.

MOTS-CLÉS. systèmes d'information, données, sécurité, intégrité, analyse multimodale, frugalité, IA.
KEYWORDS. information systems, responsible IS, data, security, integrity, multimodal analysis, frugality, AI.

1. Introduction[1]

Le Forum Jeunes Chercheuses Jeunes Chercheurs (JCJC) d'Inforsid 2024 s'est tenu à Nancy lors du congrès annuel de l'association Inforsid. Cet événement bisannuel offre aux doctorant(e)s de première ou deuxième année de thèse l'opportunité de présenter leurs travaux à l'ensemble de la communauté française de recherche spécialisée en systèmes d'information. Cet événement important pour la communauté permet de découvrir via les doctorant(e)s, une vue générale des travaux en cours dans les différentes équipes de recherche liés à la communauté Inforsid. La treizième édition du Forum n'a pas dérogé à cette tradition, avec treize doctorant(e)s présentant leurs travaux en session plénière, représentant neuf équipes de recherche françaises.

Lors de cette édition, l'essor de l'intelligence artificielle s'est fait fortement ressentir dans les présentations de différents travaux, notamment comme outil pour la gestion, le traitement et l'utilisation de données très variées (ex. publications scientifiques, scènes vidéos, séquences sémantiques temporelles, charge de travail des infirmières, dessins techniques aéronautiques, ...). La

[1] Mario CORTES CORNAX

communauté se pose de plus la question de l'impact de l'IA dans les méthodes d'apprentissage et l'enseignement.

Les treize travaux présentés reflètent comment la communauté Inforsid est de plus en plus engagée dans la responsabilité des systèmes d'informations en terme sociétal et environnemental. Nous observons aussi une inter-disciplinarité croissante dans les thèmes proposés. Des questions critiques sont abordées telles que la gestion frugale des données, la potentielle fragilité des systèmes de sécurité, l'impact de la collecte massive de données mais aussi son exploitation dans des buts tels que la détection de l'objectification dans les scènes vidéos ou la détection de citations scientifiques erronées.

Cet article reprend et étend quatre des contributions présentées lors du forum JCJC. D'abord la section 2 traite de la construction d'une plateforme versatile pour la gestion du risque cyber. On intègre ici des techniques de Machine Learning (ML) avec la modélisation plus classique des données sociotechniques pour améliorer la robustesse des SI. Ensuite, la section 3 traite de la détection de citations erronées. A partir du contexte de la citation d'une publication scientifique, le but est d'identifier automatiquement des possibles incohérences avec la publication citée. L'article présente un jeu de données et deux techniques de classification prometteuses pour réaliser cette tâche. La section 4 s'intéresse à l'analyse multimodale des scènes vidéos, notamment à l'étude de l'intégration contextuelle pour une compréhension plus approfondie des situations humaines par les systèmes automatisés. Le cas d'étude se focalise notamment dans la détection d'objectification à l'écran. Finalement, dans la section 5, on s'intéresse à la caractérisation et la mise en place d'une gestion frugale de données visant à minimiser les coûts et les impacts environnementaux associés dans l'ère du Big Data. Finalement, la Section 6 conclue l'article.

2. Graphes de connaissances : Construction d'une plateforme versatile pour la gestion du risque cyber[2]

2.1. *Contexte*

La « *softwarisation* » des infrastructures d'information et communication [CHA 16], sous-tendue par l'évolution des processus métier, s'accompagne d'une expansion de leur surface d'attaque. Dans un contexte de croissance des menaces cyber, le recours aux technologies d'aide à la décision dans l'incertain, capables de détecter rapidement les menaces inconnues, est inévitable [NAN 16].

Les modèles d'apprentissage automatique (ML) pour la cybersécurité, reposant avant tout sur l'utilisation de données structurées [MAR 19], répondent partiellement à ce besoin : pour la protection contre les logiciels malveillants par exemple, les méthodes basées sur des architectures neuronales (MLP) ont dépassé les performances des heuristiques [ASL 20] ; pour la détection d'anomalies réseaux, les méthodes nonsupervisées sont plus efficaces que les modèles d'inférence asymptomatique [SHA 18]. Cependant, si l'on se positionne d'un point de vue des systèmes d'information (SI) [TIS 15], c'est-à-dire d'un problème de décision *sociotechnique* dans l'incertain, la capture de l'information et de la connaissance « abstraite » par ces modèles manque pour supporter la décision de manière plus complète. Ces données sociotechniques résultent d'un agrégat de données techniques (*ex.* journaux d'évènements, octets de signature d'un exécutable) et de données sociologiques (*ex.* âge, hiérarchie, contexte géopolitique, *etc*).

Enfin, le recours à des solutions d'apprentissage pour la sécurité permet de répondre aux carences des organisations en ressources humaines formées à la cybersécurité. Compte tenu des immenses dégâts économiques et sociétaux causés par les cyberattaques et des progrès récents de l'apprentissage automatique, l'intérêt pour l'application de ML à la construction d'une capacité de cyberdéfense autonome capable de détecter, protéger et répondre aux attaques, s'est accru ces dernières années. Il

[2] par Marin FRANCOIS

n'existe pas de définition unique de la cyberdéfense autonome, mais à son niveau le plus élémentaire, ces agents accompliraient certaines des tâches de cyberdéfense, en protégeant les réseaux et les systèmes, en détectant les activités malveillantes et en réagissant aux comportements anormaux ou malveillants.

2.2. *État de l'art*

Les récentes avancées en modélisation des connaissances ont ouvert la porte à un nouveau champ d'application de ML [LIU 22] où, à partir d'une ontologie (graphes sémantiques et graphes de connaissances), il est possible d'intégrer des données sociotechniques non structurées dans le raisonnement d'apprentissage. Ainsi, nous nous positionnons dans la continuité des recherches existantes sur l'utilisation des modèles de ML sur graphes de connaissance pour le traitement des données sociotechniques dans le cadre de la cyberdéfense autonome des SI.

2.2.1. *Gestion du risque par la vulnérabilité*

En matière de sécurité informatique, la gestion des vulnérabilités est le processus d'identification, d'analyse et de correction des vulnérabilités exploitables par un attaquant. Pour supporter la priorisation des correctifs, les organisations s'appuient sur des indices comme *Common Vulnerability Scoring System* (CVSS) offrant une valeur d'exploitabilité et d'impact théoriques d'une vulnérabilité, représentés par les vecteurs dits « *de base* » – qui représente les caractéristiques techniques de la vulnérabilité et « *de temps* » – qui permet de tracer son évolution. L'état de l'art pour la mesure d'exploitabilité est le système EPSS (*Exploit Prediction Scoring System*) [JAC 21], qui permet de quantifier la probabilité qu'une vulnérabilité soit exploitée dans les 30 prochains jours au regard de renseignement sur les cybermenaces et de la typologie de la vulnérabilité. Cependant, EPSS ou CVSS ne permettent pas l'analyse de chaînes logiques d'exploitation de plusieurs vulnérabilités, également appelées « chemins d'attaque ». Par ailleurs, les spécificités locales (sur le plan sociotechnique) propres à l'environnement d'exploitation de la vulnérabilité, ne sont pas prises en compte dans ces indices. Ainsi, il convient de s'interroger sur la faisabilité d'une métrique de risque – similaire à la mesure d'exploitabilité, adaptée au chemins d'attaque, prenant en compte les données sociotechniques propres à l'environnement d'exploitation.

Nous avons analysé l'état de l'art en matière d'analyse des chemins d'attaque [FRA 23], de modélisation des réseaux informatiques et de modélisation du comportement des attaquants et identifié une opportunité pour de nouveaux algorithmes de modélisation des risques qui prennent en compte l'exploitation technique, les schémas d'attaque et l'environnement local. Nous nous focalisons sur trois domaines d'application : « *Digital Shadows* » (DS) [HOL 21], [DAR 22], [ECK 19], [KRI 18] et « *Digital Twins* » (DT) [HOM 23], [SUH 23], [ALL 23], [COP 23], [DIE 20], [EMP 22] pour la cybersécurité - les limites de ces derniers et notions communes avec les Graphes de Connaissances Cyber (CSKG) [LIU 22], [ZHA 20], [AGR 23], [DAS 21], [HON 23], [VAS 21], l'analyse et la modélisation des schémas d'attaque par DS et DT - y compris les applications de *Graph Machine Learning* (GML) pour l'analyse de la propagation des risques [TAK 23], [SUB 19], [HOL 21], [DAR 22] et l'utilisation de CSKG comme systèmes d'apprentissage [LUH 20], [SAL 19].

2.2.2. *Digital Shadows (DS), Digital Twins (DT), Digital Models (DM)*

Selon Eckhart [ECK 19] et Kritzinger [KRI 18], un DS est un modèle qui reçoit *automatiquement* des données de modélisation du système physique qu'il représente, mais qui n'a pas la capacité d'interagir avec ce système, contrairement au DT, qui a cette capacité. Le DS est ainsi limité à la « lecture » automatisée du modèle physique. Un DM, contrairement au DT et au DS, est une représentation non automatisée d'un système physique. Il implique une intégration manuelle des données du système physique qu'il représente et, comme le DS, n'offre pas d'interaction automatisée vers le système physique.

La quasi-totalité des travaux traitant de l'utilisation des DT pour la sécurité sont focalisés sur les environnements de Technologie Opérationnelle (OT), et ce en raison de leurs exigences de haute disponibilité que les opérations typiques de gestion des vulnérabilités (*ex. scanning*) pourraient mettre en péril. Eckart *et al.* [ECK 19] soutiennent que la recherche future en matière de DT orientée vers la cybersécurité devrait se concentrer sur l'utilisation de DT pour la conception sécurisée de Systèmes Cyber Physiques (CPS), en mettant l'accent sur l'acquisition de données de capteurs IoT. Ils suggèrent d'explorer DT pour la détection des intrusions en surveillant les Contrôleurs Logiques Programmables (PLC) et en analysant les mauvaises configurations matérielles et logicielles. D'autres auteurs [HOM 23] proposent l'utilisation de DT pour la conception sécurisée et les tests d'intrusion en environnements OT.

Les DT sont également proposés comme plateformes de support à l'Investigation Numérique et Réponse aux Incidents (DFIR). Dans [SUH 23], Suhail propose une plateforme d'attaque basée sur DT. Dans [ALL 23], les auteurs s'attachent à tirer parti du modèle pour améliorer le développement de procédures de réponse aux incidents. Cette approche est mobilisée dans [EMP 22], où les auteurs proposent une mise en œuvre axée sur l'IoT d'un système d'orchestration de la réponse aux incidents (SOAR) sur DT, ou encore dans [COP 23], où les auteurs définissent une architecture de supervision réseau basée sur DT. Enfin, Dietz *et al.* proposent l'utilisation de DT comme plateforme de support Security Operations Center (SOC) [DIE 20] et la simulation d'attaque [DIE 21] en environnement OT.

Si les travaux mentionnés offre un aperçu des capacités de modélisation des infrastructures et des comportements d'attaquants des DT/DS/DM, la question de l'intégration des données sociotechniques à ces modèles reste ouverte.

2.2.3. *Graphes de connaissances (KG), Graphes de Connaissances Cyber (CSKG) et Ontologies*

Hogan [HOG 21] définit un Graphe de Connaissances (KG) comme une « base de connaissances sémantiques structurée utilisée pour décrire symboliquement des concepts et leurs relations dans le monde physique ». Dans [LIU 22], Liu *et al.* définissent formellement un KG comme $G = \langle V, E \rangle$, où G est un multi-graphe étiqueté et dirigé, $E = \{e_1, e_2, \ldots, e_{|E|}\}$ et $V = \{v_1, v_2, \ldots, v_{|R|}\}$ sont les ensembles d'entités et de relations, respectivement. $|E|$ et $|V|$ indiquent le nombre d'éléments dans les ensembles. Dans cette définition, chaque triplet $T = \{(e, v, e') \mid e, e' \in E, v \in V\}$, représentant une relation v de l'entité de tête e à l'entité de queue e', sous la forme $\langle entité, relation, entité \rangle$ ou $\langle concept, attribut, valeur \rangle$. Les entités du KG englobent les catégories, les types d'objets et les collections, tandis que les relations établissent des liens entre les entités, formant une structure graphique. Un Graphe de Connaissances Cyber (CSKG) est un KG spécialisé pour le domaine de la sécurité, offrant une approche de modélisation intuitive pour divers scénarios d'attaque et de défense dans le monde réel.

L'ontologie est une branche de la philosophie qui traite de la nature et de l'organisation des choses. Dans les systèmes d'information, une ontologie est un modèle de données contenant des concepts et relations permettant de modéliser un ensemble de connaissances dans un domaine donné. Dans le contexte de la sécurité de l'information, on peut parler de cyber ontologie ou d'ontologie de la cybersécurité.

Dans [ZHA 20], Zhang *et al.* présentent une revue des CSKG pour l'évaluation des risques. Dans [AGR 23], les auteurs présentent une CSKG pour l'acquisition de connaissances par les analystes SOC et la gestion des vulnérabilités. Dans [LIU 22], *Liu et al.* fournissent une revue systématique des ontologies pour les CSKG. Dans [HON 23], Hong présente une méthode de détection des menaces internes utilisant un CSKG.

2.2.4. *Graph Machine Learning et CSKG pour la gestion du risque cyber*

Plus qu'un moyen efficace de représenter les données sémantiques, les CSKG offrent une structure de données qui permet l'utilisation d'algorithmes graphiques pour des structures de données qui

seraient autrement difficiles à traiter. En particulier, les algorithmes d'apprentissage automatique des graphes (GML).

Dans [DAS 21], les auteurs proposent un réseau de neurones convolutionnel graphique (GCN) pour évaluer l'importance des triplets sémantiques dans un graphe en utilisant UCO, l'ontologie unifiée cyber [SYE 16]. UCO est une ontologie spécifique au domaine de la cybersécurité. Dans [LI 23], Li *et al.* introduisent un modèle basé sur les transformeurs pour évaluer la qualité de l'ontologie et de l'intégration des données dans un CSKG. Nous avons identifié que la plupart des articles utilisant du GML pour les CSKG exploitent les propriétés graphiques des CSKG de telle manière qu'il est possible de les étendre aux hybrides CSKG-DT, comme nous le montrerons dans les prochaines sections. Les solutions analytiques s'appliquent également aux CSKG. Dans [VAS 21], Vassilev *et al.* proposent un cadre holistique pour l'analyse logique des renseignements sur les menaces et l'identification de la validation de la politique de sécurité au sein d'une organisation. Les auteurs de [DAR 22] se concentrent également sur l'exploitation des algorithmes graphiques pour contextualiser les vulnérabilités via un CSKG. Dans [TAK 23], Takko *et al.* propose une utilisation de CSKG pour l'analyse de la propagation des risques.

De facto, les graphes de connaisance sont des modèles de données très efficaces qui peuvent être exploités à l'aide d'algorithmes graphiques avec ou sans apprentissage. La structure flexible induite par les triplets permet de traiter des données sociotechniques semi-structurées. La seule condition préalable étant la construction rigoureuse d'une ontologie pour les applications spécifiques à un domaine, ces modèles de données sont à la fois polyvalents et extrêmement flexibles.

2.3. *Problématique*

Nous proposons de répondre à la problématique suivante : comment l'utilisation d'architectures CSKG-DT permet-elle intégrer les données sociotechniques à l'analyse de chemin d'attaque pour la construction d'une plateforme cyberdéfense autonome ?

Nous souhaitons proposer une plateforme modulaire, permettant de travailler dans un premier temps sur un DM, plus simple et moins coûteux à implémenter, transformé progressivement en DS puis en DT. L'objectif final de cette plateforme est de supporter des applications de cyberdéfense autonome [LOH 23]. Le but de cette recherche est donc double. D'une part la construction d'une architecture système pour l'extraction, la transformation et le traitement des données sociotechniques, d'autre part la construction d'applications pour l'aide à la décision exploitant ces données sociotechniques.

2.4. *Actions réalisées*

Nous avons implémenté partiellement cette plateforme (Figure 1). Celle-ci a pour principale fonctionnalité l'agrégation de plusieurs bases de données (BDD) relationnelles en un graphe de connaissances cyber (CSKG).

2.4.1. *Architecture du pipeline DM*

A partir du lac de données de l'organisation (1), nous utilisons un ensemble de requêtes pour formater les données selon notre propre ontologie (2). Cette ontologie permet de modéliser le réseau informatique et d'enrichir ces informations d'un graphe sémantique (3), sous forme d'un hybride CSKG-DM. Pour ce faire, nous avons modifié l'ontologie STUCCO [IAN 15], composée de 15 entités initiales et de 20 types de relations. Nous avons complété cette ontologie avec 5 nouvelles entités et 36 nouveaux types de relations pertinents pour le DM. Nous avons ensuite implémenté 18 nouvelles entités et 37 nouveaux types de relations pour représenter les schémas d'attaque. A ce stade, les données sont manipulées manuellement, ce qui correspond à la définition d'un DM. Le CSKG ainsi généré est extrait par un programme d'échantillonnage (4) qui – à partir du CSKG principal, génère de multiple sous-graphes (4) correspondants à des scénarios d'attaque précis, sur lesquels nous appliquons

un algorithme de parcours de chemins (5). Les résultats de cet algorithme sont ensuite utilisés pour entraîner un modèle d'apprentissage par induction (6), visant à généraliser les patterns propres à chaque sous-graphe (7).

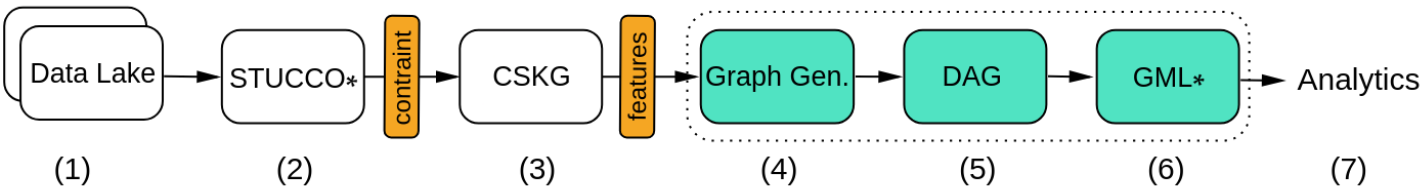

Figure 1. *Plateforme Graphe-ETL avec apprentissage sur DM*

2.4.2. *Applications du pipeline DM*

Deux applications aujourd'hui sont supportées par cette plateforme. La première (7) est basée sur un modèle de Markov Caché (HMM) [FRA 24b] permettant d'identifier le régime d'intensité de l'activité cyber. En analysant plusieurs sources d'alertes, le modèle infère le régime de perturbation dans lequel se trouve le réseau parmi trois seuils : stable, dégradé, ou critique. Les alertes sont liées à des entités du graphe : organisation(s), utilisateurs, etc. Sur cette base, nous sommes en mesure de fournir sept métriques de résilience du réseau. Le modèle proposé atteint un score F1 de 98% sur la catégorisation des alertes menant à une dégradation 1h avant celle-ci. Nous avons également proposé une méthode d'amélioration de la robustesse de ce modèle face aux attaques adverses, par exemple dans le cas ou un attaquant chercherait à perturber le modèle de détection. Notre approche est fondée sur l'apprentissage causale et applicable à tout *IDS utilisant de l'apprentissage profond. Nous avons observé une amélioration significative (+10%) des performances pour ce modèle ainsi que pour d'autres modèles état de l'art. Voir [FRA 25] pour plus d'informations.

La seconde [FRA 24a] permet d'étendre la logique du score d'exploitabilité technique (EPSS) à l'intégralité des composants du SI : données, utilisateurs, organisation(s). Nous avons proposé trois architectures permettant soit : (1) de prédire le chemin d'attaque complet entre un point d'accès initial (*ex.* un utilisateur compromis) et un point d'impact (*ex.* un serveur spécifique), (2) de prédire le point d'accès initial à partir du point d'impact, soit (3) de prédire le point d'impact à partir du point d'accès initial. Nous utilisons pour cela une mécanisme d'apprentissage profond dit « basé sur les modèles » et des convolutions sur graphe permettant d'exploiter efficacement le CSKG. Nos trois modèles offrent respectivement un score F1 de 93%, 97% et 82%. Voir [FRA 24a] pour plus d'informations.

2.4.3. *Architecture du pipeline DS*

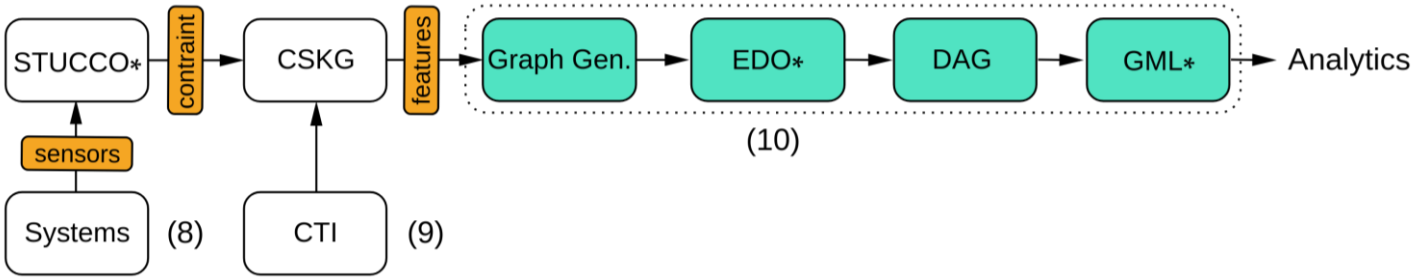

Figure 2. *Plateforme Graphe-ETL avec apprentissage sur DS*

La seconde version de la plateforme (Figure 2) transforme le modèle initial (DM) en DS. Les données sont chargées automatiquement depuis les systèmes (8), les informations de CTI (9) sont téléchargées directement à partir d'un serveur dédié, et intégrées au CSKG. Nous avons également pour objectif de modifier l'algorithme de génération des sous-graphes (10) pour exploiter un algorithme génétique (EDO) [GOE 23] permettant de maximiser la diversité des caractéristiques des

sous graphes. Cette approche permettrait d'obtenir de meilleures performances sur les modèles d'apprentissage GML. Nous avons également modifié l'algorithme de génération de graphes d'attaque. Celui-ci utilise désormais les ordonnanceurs d'attaques de MITRE CALDERA afin de simuler sur des profils d'attaquants précis. A ce stade, les artefacts générés ne sont utilisées que pour l'analyse des chemins d'attaque en fonction d'un ensemble de tactiques, techniques et procédures (TTP). Cependant, cette implémentation ouvre la porte à l'utilisation des journaux d'évènement associés pour la prochaine itération de notre plateforme.

2.5. *Actions futures*

La prochaine et dernière itération apportée à la plateforme (Figure 3) consiste à transformer le DS en DT. Pour cela, il faut que le modèle d'apprentissage ou toute autre application supportée par la plateforme ait la capacité d'interagir avec le CSKG pour entraîner une modification concrète sur le SI.

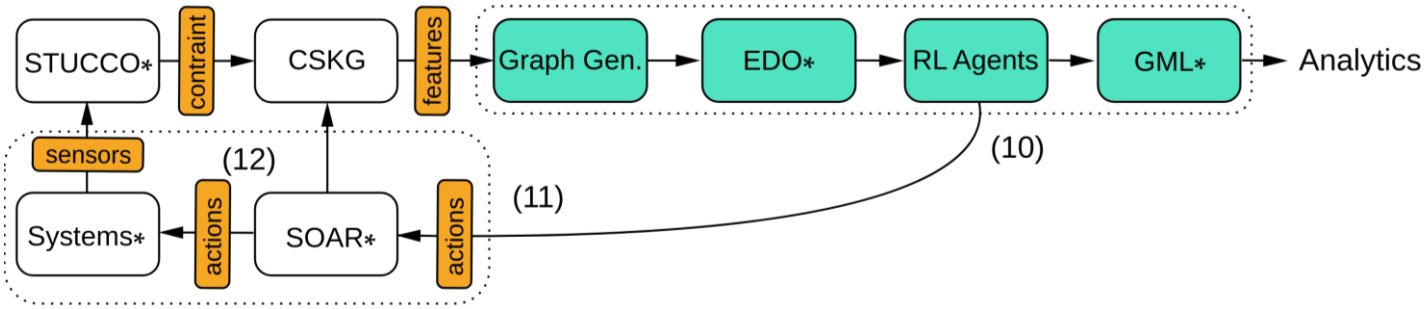

Figure 3. *Plateforme Graphe-ETL avec capacité d'interaction DT*

Pour ce faire, nous avons pour objectif d'implémenter deux agents d'apprentissage par renforcement, comme suggéré dans les travaux de [GOE 23] [NGO 23] [AGL 22]. Dans cette architecture, l'ordonnanceur est remplacé par un agent d'apprentissage par renforcement offensif (10). L'environnement d'apprentissage est donné par un sous-graphe du CSKG, les actions de l'agent sont contraintes par les TTP correspondant au profil de l'attaquant. Les récompenses sont définies par un opérateur humain en charge de l'analyse de risque.

A ce stade de notre recherche, nous avons expérimenté l'apprentissage par renforcement (via *Q-Learning*) et par renforcement profond (via DQN) pour l'agent offensif. Celui-ci est d'ores et déjà en capacité de répliquer les chemins d'attaque proposés par plusieurs ordonnanceurs. Face à cet agent offensif, un second agent est entraîné (10). Son rôle est de sélectionner un ensemble de contre-mesures applicables au sous-graphe observé. L'espace d'action utilisable est défini par les ressources disponibles au sein de l'organisation. Elles peuvent par exemple correspondre à l'application de mesures de protection (règles de pare-feu, isolement, *etc.*) ou de détection (positionnement de leurres afin de maximiser une récompense liée à l'identification de l'ensemble de TTP utilisé par l'agent offensif). Une fois ces deux agents entraînés, nous souhaitons recourir à un connecteur permettant de lier l'agent défensif directement à l'environnement de production. Par l'intermédiaire du serveur d'orchestration (SOAR), celui-ci aurait la capacité d'analyser en temps réel les journaux d'évènements et les informations présentes dans le CSKG pour assurer son rôle de cyberdéfense autonome.

2.6. *Conclusions*

Dans ce chapitre, nous avons présenté une plateforme d'extraction, transformation, chargement des données en graphes pour la sécurité des systèmes d'information. Cette architecture permet à une organisation de construire sur le long terme une capacité d'apprentissage sur données sociotechniques, qu'il serait difficile d'intégrer sans recourir au modèle de données proposé. Par ailleurs, cette architecture de traitement permet de « recycler » les données, réalisant ainsi des économies d'échelle : les applications existantes et celles proposées, bien qu'ayant des routines de traitement différentes, utilisent ce même modèle de données et sont complémentaires. Par exemple, nous pouvons appliquer la

routine d'inférence de régime en tenant compte de la topologie de l'infrastructure et l'espacement géographique. L'organisation se positionne ainsi en capacité d'améliorer sa prise de décision dans l'incertain, notamment pour l'identification des risques, la protection des actifs, la détection des menaces, et la réponse dynamique aux menaces.

3. Détection automatique de citations erronées : jeu de données et méthodes3

3.1. *Contexte*

Les citations jouent un rôle important dans la recherche scientifique. L'utilisation des citations dans les articles scientifiques est une pratique essentielle qui sert à différents objectifs pour les auteurs. Par exemple, les citations sont utilisées pour établir le contexte de recherche, référencer des méthodologies ou mettre en évidence des résultats ou des théories contrastés [JUR 19]. Cependant, de nombreuses citations erronées sont identifiées au sein des publications scientifiques. Ces citations erronées, également appelées miscitations, peuvent conduire à une mauvaise interprétation des recherches citées, à une distorsion du message que l'auteur original souhaitait transmettre, et, potentiellement, à la propagation d'erreur dans la littérature scientifique.

Certaines recherches existantes ont déjà commencé à catégoriser les erreurs de citation. Une étude [GLE 19] a évalué les contextes de citations faisant référence à leur publication sur les tailles de « focus group » [GLE 11]. Une autre étude [LAC 85] a classé les erreurs de citation en trois catégories : les erreurs triviales, les erreurs légèrement trompeuses, et les erreurs graves.

Inspiré par ces études, nous avons d'abord découvert dans certains articles les citations erronées hors-sujet. Ces citations erronées n'ont aucune pertinence par rapport aux idées exprimées dans l'article cité, et elles concernent également un sujet de recherche différent de celui de l'article référencé. [La table 1 donne un exemple d'article de science de l'ingénieur qui cite de manière aberrante un article de biologie animal]. L'objectif de notre recherche est de détecter automatiquement ce type de citations aberrante à partir du contexte de citation et deconstruire un jeu de données contenant ces citations erronées et des citations fiables. Nous avons d'abord construit manuellement un jeu de données équilibré, contenant à la fois 99 citations erronées et 100 fiables dans les articles scientifiques de différents sujets (biologie animale, biologie moléculaire, sociologie, informatique etc.). Ce jeu de données vise à tester la faisabilité de notre recherche. Ensuite, nous avons défini deux configurations sur l'abstract de l'article cité : la configuration abstract entier et la configuration abstract segmenté. Pour chaque configuration, nous avons utilisé deux méthodes de classification pour déterminer les citations fiables et erronées : la méthode de similarité cosinus et la méthode de classification par paraphrase.

Selon nos résultats expérimentaux préliminaires, la similarité cosinus offre les meilleures performances sur notre jeu de données. Avec nos méthodes et le jeu de données équilibrés, nous démontrons la faisabilité de notre recherche et nous sommes actuellement en train de constituer automatiquement un jeu de données plus large.

3.2. *État de l'art*

Il existe déjà des recherches sur les citations dans les articles scientifiques. Certaines de ces recherches se concentrent sur la réalisation d'analyses statistiques des citations erronées, tandis que d'autres études se consacrent à l'analyse des citations en utilisant des techniques de traitement du langage (TAL).

[3] Qinyue LIU

Certaines recherches sur les citations se concentrent sur la quantification de la fréquence des citations erronées. Dans une étude sur les citations parue dans OHNS, 50 références aléatoires ont été analysées, révélant des erreurs dans 17% des cas, dont 34% considérées en tant qu'erreurs majeures [ARM 18]. Il y a également des chercheurs qui ont analysé le contexte des citations pour identifier les tendances dans les sciences biomédicales [JEB 21]. Une autre recherche a développé une méthode pour étudier les thèmes cachés dans les publications, en analysant les résumés et les citations d'un article source [LIU 13].

D'autres études utilisant des techniques de TAL se sont consacrées à diverses tâches analytiques. Une étude a analysé le sentiment des citations [LIU 17]. Dans leur travail, les auteurs ont défini trois classes de sentiments pour les citations dans leur ensemble de données, ce qui est extrait de l'ACL (Anthology Reference Corpus [BIR 08]). Ils ont défini trois catégories de sentiment pour les contextes de citation : "N" indique un sentiment négatif, "P" un sentiment positif, et "O" un sentiment objectif. Cette analyse de sentiment vise à distinguer les citations selon ces trois classes.

Une autre étude propose la classification de la polarité des citations [BOR 22]. Ils ont adapté (fine-tuned) différents modèles de langage pour classifier les contextes critiques et non critiques. En utilisant les corpus CitaNeg et Critical Contexts [TE 22], les chercheurs ont construit leur propre corpus. Dans ce corpus, les citations positives et neutres de CitaNeg ont été considérées comme non critiques, tandis que celles provenant du Critical Contexts Corpus ont été classées comme critiques.

3.3. *Problématique*

De nombreuses études antérieures ont utilisé des techniques de TAL pour l'analyse des citations. Cependant, peu de recherches se sont concentrées sur l'évaluation automatique de la fiabilité des citations. Il n'y a également pas suffisamment de jeu de données pour l'évaluation des citations. La collection de ces données n'est pas une tâche facile, car le procès d'annotation peut être assez longue.

À cet égard, notre étude vise à distinguer automatiquement les citations fiables et les citations erronées. Pour ceci, nous constituons un jeu de données en collectant des exemples de différents types de citations, et testons différentes méthodes de TAL pour classifier automatiquement les citations.

3.4. *Actions réalisées*

Nous avons d'abord collecté des citations fiables et erronées dans les articles scientifiques pour constituer un ensemble de données de test. Ensuite, nous avons défini deux configurations. Pour chaque configuration, nous avons utilisé deux méthodes de classification pour déterminer les citations fiables et erronées : la méthode de similarité cosinus et la méthode de classification par paraphrase (Figure 4). Dans nos expériences, nous nous concentrons sur l'évaluation de la similarité entre le contexte de la citation dans les articles citant et la section de l'abstract dans les articles cités.

3.4.1. *Jeu de test*

Une citation est considérée comme non fiable si un contexte justifiant est absent dans l'article cité ou si le contexte de l'article cité ne soutient pas la citation. Inversement, une citation est considérée comme fiable si elle est soutenue par un contexte dans l'article cité qui justifie son utilisation (Table 1). Cette classification binaire correspond à une simplification du problème général beaucoup plus complexe qui consiste à savoir si le contexte de citation reflète bien le contenu de l'article cité.

Les contextes de citation ont été collectés et annotés manuellement à partir des articles en libre accès qui citaient six articles de différents domaines scientifiques (biologie animale, biologie moléculaire, sociologie, informatique etc.) . Trois de ces articles sont connus pour « attirer » les citations erronées. Nous avons d'abord lu l'abstract de chacun de ces six articles, puis extrait les contextes de citation des articles qui ont cité ces 6 articles. Chaque contexte de citation a ensuite été évalué et annoté en le

comparant avec l'abstract de l'article cité. Au total, 199 citations ont été collectées pour le jeu de données. Pour garantir l'équilibre, 100 de ces citations sont fiables, tandis que 99 sont erronées.

Catégorie	Contexte de citation	*Abstract* d'article cité
Fiable	*For instance, other approaches for topic modelling can be tested.*	*Semantic similarity detection is a fundamental task in natural language understanding. Adding topic information has been useful for previous feature-engineered semantic similarity models, as well as neural models for other tasks.* **[PEI 20]**
Erronée	*Eddy covariance devices or lysimeters can be used to determine ET0*	*Male moths compete to arrive first at a female releasing pheromone. A new study reveals that additional pheromone cues released only by younger females may prompt males to avoid them in favor of older but more fecund females.* **[VIC 17]**

Table 1. *Exemples de citation fiable et de citation erronée*

3.4.1. *Configurations*

Configuration de l'intégralité de l'abstract : Dans cette configuration, nous extrayons le texte complet de la section de l'abstract de l'article cité sans apporter de modifications. Nous traitons l'intégralité de l'abstract, composé de plusieurs phrases, comme un seul document. Ensuite, nous associons l'abstract entier avec le contexte de citation de l'article citant pour mesurer leur corrélation.

Configuration de l'abstract segmenté : Dans un premier temps, la section de l'abstract de l'article cité est segmentée en phrases individuelles. Ensuite, chaque phrase est associée au contexte de citation. Par exemple, si un abstract est composé de 5 phrases, chaque phrase de l'abstract est alors associé avec le contexte de citation de l'article citant. Ce processus crée 5 paires de citations et abstract. Ces paires représentent collectivement la relation entre le contexte de citation et l'intégralité de l'abstract. En utilisant ces paires (contexte de citation, phrase), nous évaluons ensuite la corrélation entre le contexte de citation et l'abstract de l'article cité.

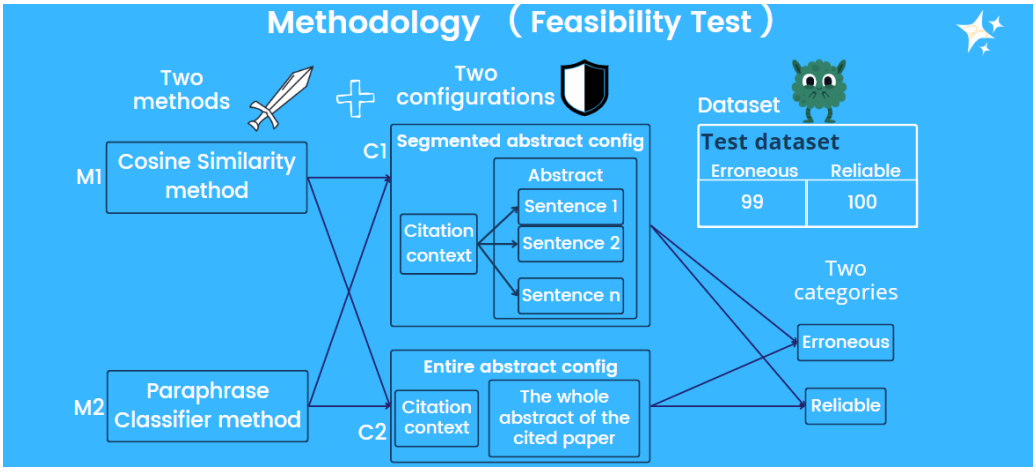

Figure 4. *Les configurations et les méthodes*

3.4.2. *Méthodes pour classifier les citations*

Similarité Cosinus : La similarité cosinus est largement utilisée pour mesurer la similarité entre deux textes sous formes de vecteurs (plongements qui capturent le contenu sémantique). Nous avons utilisé le modèle BERT [DEV 18] pour générer les plongements du contexte de citation et de l'abstract d'article cité et comparer leurs similarités.

Avec la configuration de l'abstract entier, nous calculons directement la similarité cosinus entre le contexte de citation et l'abstract entier dans les articles référencés.

Avec la configuration de l'abstract segmenté, nous segmentons un abstract en plusieurs phrases, puis, nous calculons la similarité entre le contexte de citation et chaque phrase segmenté de l'abstract. Nous sélectionnons la paire qui à la plus haute similarité pour représenter globalement la similarité entre le contexte de citation et l'abstract.

Basé sur l'analyse de la courbe « Receiver Operating Characteristic (ROC) [HAN 89] », nous établissons un seuil de 0.75 pour différencier les citations fiables et les citations erronées.

Classifieur de paraphrase : Nous avons adapté (fine-tuned) un classifieur également basé sur BERT [DEV 18] en utilisant le corpus MSRP pour différencier les citations fiables et erronées. La sortie du classifieur est catégorisée soit comme 'paraphrase', soit comme 'non paraphrase'. Dans notre cas, une sortie 'paraphrase' signifie une citation fiable ; Une sortie 'non paraphrase' signifie une citation erronée.

Dans la configuration de l'abstract segmenté, nous évaluons la proportion de l'abstract qui est classée comme une paraphrase du contexte de citation. Par exemple, si un résumé est segmenté en 5 phrases et que notre classifieur identifie 2 de ces phrases comme des paraphrases du contexte de citation, nous en déduisons alors que 40 % (2 sur 5) de l'abstract est considéré comme une paraphrase du contexte de citation, et donc fiable.

Basé sur l'analyse de la courbe ROC (Receiver Operating Characteristic) [HAN 89], pour minimiser les xx et maximiser les xxx nous avons établi un seuil de 11 %. Cela signifie que si plus de 11 % d'un abstract est identifié comme une paraphrase du contexte de citation, alors la citation est considérée comme fiable.

3.4.3. *Collection automatique des citations*

Comme mentionné dans la section précédente, nous avons collecté manuellement les citations pour tester nos méthodes et configurations. Cependant, nous avons pensé qu'il était nécessaire de développer un script pour collecter automatiquement des citations à partir des titres d'articles ou de journaux scientifiques.

Notre script extrait les citations depuis la base de données « Elsevier » et recherche les abstracts associés à ces citations dans les bases de données « Elsevier » et « CrossRef » via un token API[4]. Lorsqu'un nom de journal scientifique est fourni, notre script génère automatiquement un fichier contenant les contextes des citations, les abstracts référencés trouvés, ainsi que d'autres métadonnées. Le script extrait les citations des articles les plus récents du journal spécifié par l'utilisateur.

3.5. *Actions futures*

Dans cette étude, notre objectif principal est d'évaluer la fiabilité des citations dans les articles scientifiques. Nous avons construit un jeu de données comprenant 199 contextes de citation, proposé et évalué deux méthodes avec deux configurations sur nos données. La méthode de Similarité Cosinus a donné de meilleurs résultats avec les deux configurations, atteignant une précision de 93% sur notre jeu de données. La méthode de classifieur a atteint une précision de 87.4% avec la configuration de l'abstract segmenté, et une précision de 66.3% avec la configuration de l'abstract entier. Notre résultat a prouvé la faisabilité de notre recherche.

[4] https://api.crossref.org/swagger-ui/index.html
https://dev.elsevier.com

Pour les travaux futurs, nous envisageons d'ajouter d'autres types de citations erronées et d'agrandir le jeu de données. Nous pensions à raffiner notre script pour collecter automatiquement les citations afin d'agrandir le jeu de données.

Nous souhaiterions également tester nos méthodes sur des articles scientifiques où le nombre de citations fiables dépasse celui des citations erronées, plutôt que tester sur notre jeu de données équilibré. De plus, nous envisageons de mener une recherche statistique pour évaluer si la section abstract d'un article cité suffit à justifier le contexte de citation dans l'article citant. Cette analyse aiderait à déterminer s'il est nécessaire d'analyser l'ensemble de l'article cité ou si se concentrer uniquement sur la section abstract est suffisant.

4. Analyse multimodale de scène : vers une intégration des données contextuelles?[5]

4.1. *Contexte*

Les sous-domaines de l'intelligence artificielle, tels que l'apprentissage automatique, cherchent à doter les systèmes informatiques de capacités similaires à celles des humains pour des tâches spécifiques. Ces tâches peuvent impliquer une ou plusieurs modalités de communication, telles que le texte, l'image ou le son. L'apprentissage multimodal, qui permet de combiner différentes modalités pour entraîner un système automatisé, offre de nouvelles opportunités dans des domaines tels que l'analyse d'interactions, de scènes ou de publicités, avec des résultats de plus en plus encourageants [GAS 18].

Cependant, très peu d'études exploitent des modalités autres qu'une image associée à sa description et/ou un audio [VIC 18] [KUK 20], négligeant ainsi certaines informations contextuelles. Or, ne pas tenir compte du contexte pourrait entraîner une perte d'informations cruciales lors de l'analyse d'une interaction, le point de vue pouvant être influencé par exemple par le caractère formel ou non de la situation, le contexte de la scène (par exemple, une dispute légale dans un tribunal plutôt qu'une conversation houleuse dans un lieu public), de la relation entre les acteurs de l'interaction (amis, collègues, ennemis, etc.), ou des attributs spécifiques aux personnages tels que leur profession, pouvant influencer les dynamiques sociales. D'autant plus que, lors de situations sociales, le cerveau humain s'engage dans une analyse complexe des signaux sociaux, en s'appuyant sur un large éventail d'entrées sensorielles s'étendant au-delà des signaux visuels, englobant les stimuli auditifs, le contexte environnemental, sociétal, les influences culturelles et le background éducationnel ou les connaissances métiers (ex: expertise en sciences du comportement permettant d'analyser plus finement des rapports de domination), contribuant ainsi à une compréhension globale de la dynamique sociale [QOD 18] [LIU 19]. Ceci est particulièrement observable à travers la Figure 5, où différents niveaux de contexte apportent des interprétations différentes. Si l'on a deux personnages A et B, avec A qui frappe B à l'écran, l'on peut supposer qu'il s'agit d'une bagarre ou d'une agression. Si A frappe B dans un ring de boxe, avec un arbitre désigné, l'on peut plus facilement supposer qu'il s'agit d'un combat de boxe. Si A frappe B, mais que l'on sait que A et B sont des comédiens, et que la scène a lieu durant leur sketch (possiblement inféré de méta-données vidéo), on peut plus facilement supposer qu'il s'agit d'un sketch, ou encore d'une répétition. Cet exemple illustre à quel point notre compréhension peut être influencée par l'apport de contexte dans une interaction.

[5] Ibrahim MOHAMED SEROUIS

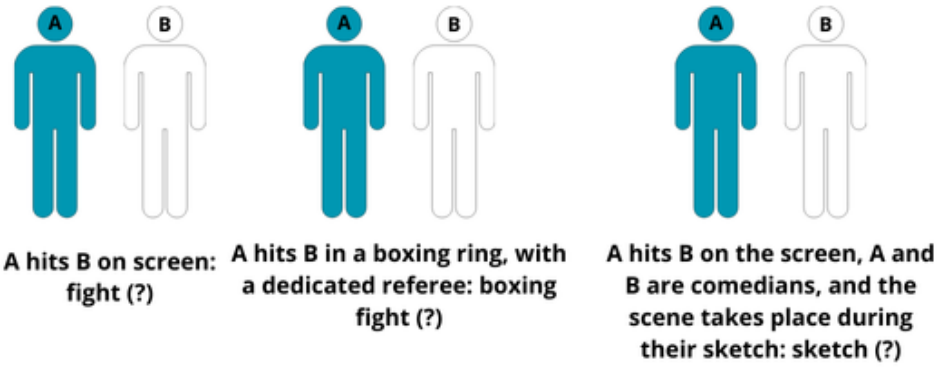

Figure 5. *Interprétation de la scène avec différents niveaux de contexte*

De plus, dans la poursuite effrénée de l'algorithme ou de la méthode ayant la plus grande précision, l'on néglige comment représenter ces données et non uniquement les utiliser dans le but de les fournir à un problème d'apprentissage.

Dans le cadre du projet ANR TRACTIVE [TRACTIVE], une collaboration interdisciplinaire de plusieurs laboratoires, nous sommes amenés à étudier les différences de représentation multimodale entre les genres masculin et féminin dans les films. Cette étude, qui s'appuiera sur des données visuelles, textuelles et annotées par des experts, vise à produire une interprétation de haut niveau de l'objectification (réduction d'un personnage à l'état d'objet de désir, de par la représentation de son corps, par le discours, ou d'autres éléments contextuels) de manière automatisée. Ce travail de recherche s'inscrit donc dans le domaine de l'analyse multimodale de scène, de manière générique, avec une application spécifique à la détection d'objectification à l'écran. Notre étude vise à ouvrir des nouvelles perspectives pour une compréhension plus approfondie des situations humaines par les systèmes automatisés.

4.2. *État de l'art*

L'analyse de scène en intelligence artificielle est un domaine de recherche en pleine expansion qui vise à comprendre et interpréter automatiquement des scènes visuelles complexes, de manière similaire aux humains. Cette compréhension implique non seulement la reconnaissance et la localisation d'objets dans une scène, mais aussi la compréhension de leurs attributs, de leurs relations spatiales et sémantiques, et même de leurs actions et interactions.

Elle trouve ses racines dans les premiers travaux sur la vision par ordinateur et la reconnaissance d'objets. Les pionniers de ce domaine tels que David Marr [MAR 10] ont commencé à explorer dans les années 80 comment les ordinateurs pouvaient interpréter et comprendre des images et des vidéos. Au cours des années 1980 et 1990, des algorithmes plus sophistiqués ont été développés pour l'analyse de scène. Ces derniers utilisaient des techniques de traitement d'image et de reconnaissance de formes pour identifier des objets et des scènes dans des images. Ensuite, l'avènement réseaux de neurones convolutifs (CNN) [LEC 98] a permis des avancées significatives dans la reconnaissance d'objets et la compréhension de scènes. Grâce aux avancées en apprentissage automatique et en vision par ordinateur, ce domaine continua de progresser et de trouver de nouvelles applications dans divers secteurs, s'étendant à une variété d'applications, y compris la conduite autonome, la surveillance vidéo, et la réalité augmentée.

En fonction de la tâche, l'analyse de scène, notamment appliquée à des situations centrées sur l'humain, est généralement réalisée à l'aide d'une de ces modalités ou une combinaison de ces modalités: données visuelles (image ou séquence d'images) [CAR 17], textuelles (sous-titres d'une vidéo, texte affiché à l'écran) [JIA 18], audio (bande-son, voix des personnages), données de radars/capteurs [DAI 17], méta-données (description narrative de la scène, contexte de la scène,

relations entre les personnages, le lieu exact de la scène, les attributs des personnages à l'écran tels que leur profession, etc).

Néanmoins, concernant les situations centrées sur l'humain, certaines données contextuelles sont très souvent négligées dans la littérature. Nous considérons pourtant vrai qu'une compréhension plus complète des interactions interpersonnelles et des situations sociales au sens large ne peut être obtenue qu'en incorporant des indices contextuels tels que le contexte de la scène ou les relations entre les personnages, pour n'en citer que quelques-uns.

4.3. *Problématique*

Dans le contexte d'application défini précédemment, plusieurs défis initiaux se posent, qui peuvent être résumés par les trois questions suivantes :

– Comment prendre en compte la dimension contextuelle dans un problème d'analyse de scène ?

– Quels sont les biais potentiels liés à l'intégration du contexte, qui peut se révéler subjectif, et comment les minimiser ?

– Quelles données utiliser et comment les représenter et les traiter de manière adéquate ?

4.4. *Actions réalisées*

4.4.1. *Modèle d'appprentissage*

Les approches basées sur les Graph Neural Networks (GNNs) sont de plus en plus populaires pour les problèmes de classification sur des données multimodales, bien que certaines réticences aient été exprimées dans la littérature [EKT 23]. Les GNNs permettent d'exploiter l'aspect relationnel entre les données et de traiter des données de tailles variables, ce qui en fait une piste intéressante à explorer pour notre problème. De plus, nous disposons de graphes de scènes provenant du jeux de données MovieGraphs [VIC 18] pour la compréhension des situations centrées sur l'humain, une collection largement reconnue comprenant 7637 scènes de 51 films, représentées sous forme de graphes orientés, présentant les informations sous formes de nœuds et leurs connexions sous forme d'arcs. Ces graphes contiennent des informations spécifiques relatives à la scène, englobant l'identité des personnages, les attributs physiques et personnels/filmiques (tels que l'âge, le nom, la taille, la profession), les relations entre les personnages, les interactions interpersonnelles, et les marqueurs chronologiques associés aux éléments de la scène.

Nous avons donc développé une méthodologie en trois étapes pour tirer parti de la richesse des données contextuelles :

1. La première étape consiste en l'encodage des données d'entrée, soit les attributs des nœuds du graphe, via un modèle d'encodage basé sur l'architecture BERT [DEL 19].
2. La deuxième étape consiste en l'apprentissage de la représentation des nœuds du graphe et de leurs connexions, via l'algorithme de passage de message [GIL 17] et des convolutions de graphes [DEF 16] autour des nœuds d'intérêt, que nous définissons comme les nœuds ayant généralement le plus de connexions dans le graphe (dans notre cas, les nœuds d'interaction, de personnages, et le nœud contenant des métadonnées sur la scène).
3. La troisième étape consiste en la classification des nœuds racine (nœuds dont on souhaite obtenir la classe). Pour résoudre le problème de boîte noire [HUS 19] associé à ce type d'algorithme, nous effectuons un calcul de la sensibilité du résultat final aux variations dans les données d'entrée, afin d'évaluer l'impact relatif de chaque type de nœud sur le résultat final. En sortie, nous avons donc à la fois la probabilité du nœud racine d'appartenir à chaque classe finale, ainsi que des scores de sensibilité.

Notre approche a été évaluée sur différentes tâches d'analyse de scène, telles que la détection d'objectification, la classification d'interactions et la détection de relations entre les personnages. Les

résultats préliminaires obtenus sont prometteurs, dépassant même ceux de [KUK 20] sur la classification de relations entre les personnages, comme illustré en dans la Table 2.

Modèle	Précision (%)	Top-2 précision (%)
LIReC	25	N.C
LIReC (avec agrégation)	28.1	N.C
Notre approche	**30.8**	**39.4**

Table 2. *Résultats préliminaires - Classification de relations sociales sur MovieGraphs*

4.4.2. *Méthode d'extraction des données*

Comme illustré dans la Figure 6, le module AMDER que nous proposons pour l'extraction des données de scène prend en entrée une vidéo et en génère en sortie un graphe de scène. Ce graphe comprend les actions effectuées par les personnages au sein de la vidéo, les discours des personnages (sans toutefois l'identification des interlocuteurs), les coordonnées de détection des personnages, ainsi que les attributs physiques des personnages (teint, sexe, vêtements), les parties du corps visibles de chaque personnage, et les expressions faciales ou émotions des personnages au cours de la scène.

Ces informations sont extraites à l'aide de blocs composés de modules, chacun ayant un rôle précis :

1. Dans le premier bloc contenant un seul module, il s'agit de la détection de changement de décor/de scène, afin de diviser la vidéo en scènes. Les traitements qui suivront vont ensuite être effectués sur chaque scène.
2. Ensuite, le deuxième bloc se charge d'extraire le discours de la scène ainsi que les indicateurs temporels via le module *speech recognition*. Un autre module du même bloc, *activity recognition*, se charge de la reconnaissance d'activités tout au long de la scène. Le dernier module, *instance detection and tracking,* se charge d'effectuer la détection et le tracking des personnages au sein de l'interaction.
3. Dans le troisième bloc, les personnages détectés et « trackés » à l'étape précédente voient leur expressions faciales analysées afin d'en extraire les possibles émotions des personnages, et des attributs physiques tels que l'appartenance ethnique et le sexe apparents sont extraits. En cas d'association d'attributs physiques multiples pour une même catégorie (appartenance ethnique, par exemple), nous associons la catégorisation avec la plus grande probabilité en moyenne sur la scène.
4. Enfin, le dernier bloc prend les différentes informations extraites dans les précédents modules afin de générer un graphe de scène tel que dans la Figure 6.

Le module global AMDER peut être utilisé comme un outil de pré-annotation, auquel on pourrait appliquer un algorithme d'analyse de relation entre les personnages, tel que celui mentionné dans la section 4.4.1 afin d'enrichir les données contextuelles avec le contexte narratif.

La sortie du module est une représentation qui s'inscrit dans une première tentative de modélisation des données relatives aux scènes. Cette modélisation inclut les personnages, leurs attributs (tels que le sexe, la race, les expressions faciales...), les coordonnées de détection, les émotions exprimées pendant la scène, l'ensemble des interactions réalisées dans une scène, des informations relatives au lieu de la scène, ainsi que le discours tenu lors de l'interaction.

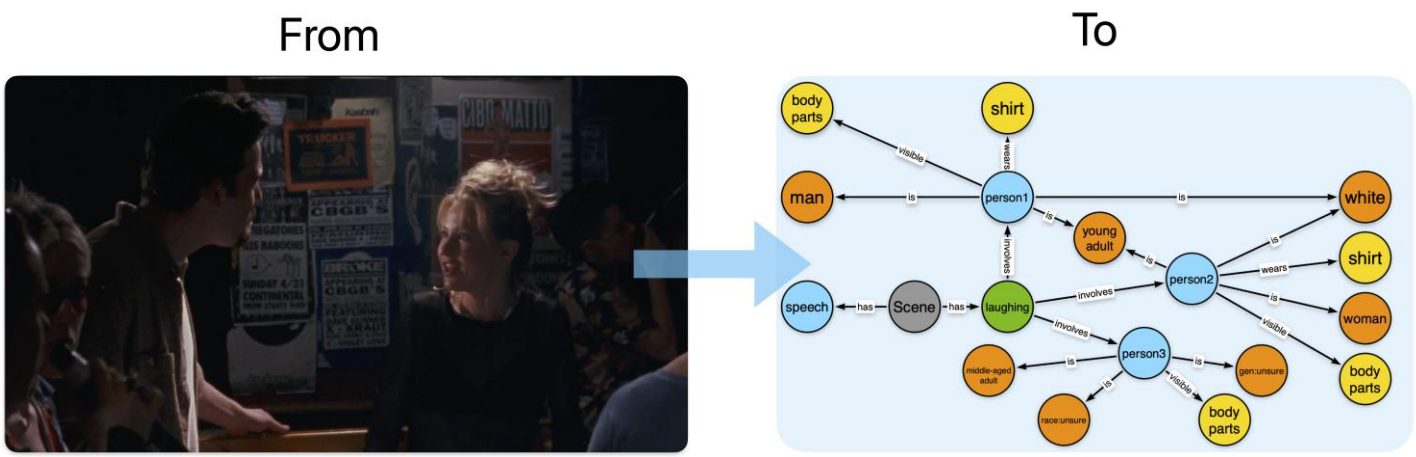

Figure 6. *Vidéo (en entrée) et graphe de scène (en sortie) du module AMDER.*

4.5. *Actions futures*

Les premiers résultats du module d'extraction des données contextuelles étant globalement encourageants concernant l'éventail de données pouvant être extrait, certains aspects du module restent perfectibles. Nous envisageons d'intégrer des techniques de Human Parsing, telles que celle proposée par [LIA 18], afin d'obtenir des détails plus fins sur les tenues vestimentaires des personnages à l'écran. Cela permettrait par exemple de détecter la nudité, ou une tenue inappropriée dans un contexte sérieux. Nous prévoyons également d'ajouter des techniques de réduction de bruit pour améliorer l'extraction du discours dans les vidéos, ainsi que l'utilisation de grands modèles de langage pour obtenir une description de la scène basée sur les éléments extraits. Cependant, une difficulté persiste dans l'évaluation objective par rapport à d'autres modules dans la littérature, la plupart se focalisant sur un problème ou une modalité précise, à l'instar de [SIV 20] qui se focalise sur les vidéos de danse ou [ASH 16] et [KIM 13] sur les données visuelles.

Bien que cette méthodologie soit plus performante que certaines méthodes de référence, telles que celle proposée par [KUK 20], pour la classification d'interactions, elle pourrait être améliorée en intégrant des connaissances métiers, en particulier pour le problème de détection d'objectification. Nous envisageons donc d'introduire une approche neuro-symbolique qui bénéficierait des retours d'experts pour la partie symbolique, et des sorties de notre modèle comme connaissances préalables.

4.6. *Conclusion*

Cette étude vise à ouvrir de nouvelles perspectives pour une compréhension plus approfondie des situations humaines par les systèmes automatisés, en intégrant les données contextuelles dans l'analyse de scènes.

Dans un premier temps, nous proposons une méthodologie d'apprentissage automatique interprétable pour les scènes, capable d'intégrer des données contextuelles (comme les relations entre les personnages et le lieu de la scène) en plus des entrées traditionnelles (images, transcriptions de discours). Basée sur l'utilisation de graphes de connaissances, cette approche a montré des résultats préliminaires prometteurs, bien qu'elle reste perfectible, notamment en ce qui concerne l'intégration de connaissances métiers pouvant apporter un niveau de contexte plus élevé.

Enfin, nous présentons un module d'extraction de données vidéo, qui peut servir de pré-annotation pour la création de jeux de données contenant des scènes. Les premiers résultats sont globalement satisfaisants, et des pistes d'évolution sont actuellement explorées pour enrichir le spectre d'informations obtenues.

À long terme, nous envisageons un avenir où de tels systèmes pourraient être utilisés à grande échelle pour l'annotation et l'analyse de scènes. Cependant, les possibles biais émanant de ces

technologies devraient être étudiés avec minutie, notamment dans des applications sensibles pouvant influencer des décisions importantes concernant des individus. Pour un exemple plus précis, l'on peut prendre le logiciel COMPAS aux États-Unis, utilisé par la justice pénale pour prédire la probabilité de récidive d'un mis en examen, qui s'est révélé biaisé à l'encontre des afro-américains, car ils étaient plus susceptibles d'être qualifiés de personnes à haut risque même s'ils n'avaient jamais été condamnés auparavant. Plus on enrichit les données relatives aux personnages ou même sur le contexte de l'interaction, plus l'on multiplie les sources de données, plus des biais de ce genre peuvent émerger. Il faudrait être capable d'identifier ces biais les catégoriser, et éventuellement les minimiser afin d'assurer une intégration adéquate.

5. La gestion frugale de données[6]

5.1. *Contexte*

L'essor du Big Data et le récent soutien du paradigme "load-first" [FAR 16] ont incité les entreprises à collecter et produire de grandes quantités de données dans l'éventualité où elles pourraient s'avérer utiles à l'avenir. En conséquence, nous sommes confrontés à une accumulation impressionnante de données redondantes et inutiles. Ainsi, les activités de traitement et de diffusion des données peuvent être associées à des niveaux élevés de complexité.

Cette approche, souvent observée dans les Data Lakes, a ses conséquences, même si elle est populaire pour sa flexibilité en termes de systèmes de stockage, de formats de données, de métadonnées et d'autonomie [NAR 19], ce qui représente un avantage économique dans certains cas, ou un désavantage économique puisqu'elle peut entraîner des coûts importants.

Dans ce contexte, en termes de conséquences environnementales, nous assistons à un gaspillage considérable de ressources, comme l'énergie, ce qui est catastrophique dans le contexte écologique actuel. Des niveaux record de consommation d'énergie continuent d'être enregistrés, car chaque opération de traitement des données consomme de l'énergie. Selon l'Agence Internationale de l'Énergie (IAE), la consommation totale d'électricité à l'échelle mondiale des centres de données pourrait atteindre plus de 1000 TWh en 2026, ce qui équivaut approximativement à la consommation d'électricité du Japon[7].

D'un point de vue sociétal, on observe une utilisation non éthique des données, notamment en ce qui concerne la collecte massive de données personnelles sans le consentement explicite des individus ou sans transparence sur les finalités de cette collecte. Cela soulève des questions importantes liées à la vie privée et à la manipulation des comportements des utilisateurs. Ces pratiques soulignent l'importance d'une réglementation stricte et d'une éthique forte dans la gestion des données.

Alors, nous sommes confrontés à un trilemme entre les aspects économiques, sociétaux et environnementaux. Ainsi, la "Frugalité" émerge comme une solution potentielle pour prévenir ces problèmes, car ce concept peut être perçu comme un "compromis" entre ces différents aspects.

5.2. *État de l'art*

"More with less" ou "Faire plus avec moins" est devenu un mantra courant dans de nombreux domaines pour exprimer l'idée d'atteindre une production plus élevée tout en utilisant moins de ressources.

---

[6] Vlada STEGARESCU

[7] https://www.iea.org/reports/electricity-2024/executive-summary

Ce concept est considéré comme prenant ses sources dans les principes de l'approche "Lean", qui provient du « Système de production Toyota »[8], principalement axé sur l'augmentation de la valeur et le centrage sur l'utilisateur tout en réduisant les déchets.

Dans cet objectif de réduction de déchets, la question de l'optimisation de ressources a été étudiée de près. D'un point de vue économique, certains travaux analysent l'optimisation de ressources dans un objectif de minimisation de coûts [ZHA 13], ou encore la réutilisation de ressources [SHA 20].

Face à l'urgence climatique, les obligations environnementales telles que les Accords de Paris exigent une réduction drastique de la consommation de ressources et des émissions de gaz à effet de serre. Dans ce contexte, l'optimisation de ressources est souvent associée avec un impact environnemental positif [SHA 20].

D'un point de vue sociétal, l'optimisation de ressources est souvent étudiée en lien avec le traitement de données à caractère personnel. La minimisation de données étant inscrite dans le Règlement Général sur la Protection des Données (RGPD) comme une des meilleures techniques de protection des données[9], elle a servi comme sujet de recherche de plusieurs travaux [ADA 19], [SHA 22], [FIN 21].

En raison du fait que ces solutions abordent un ou plusieurs des aspects économique, environnemental ou sociétal, qui sont les principes à la base de l'éco-responsabilité ou encore de la durabilité, une confusion entre les concepts "green" et la frugalité a été créée. Alors, la frugalité est souvent utilisée comme synonyme de responsabilité environnementale et de durabilité. Cependant, ces concepts ne sont pas interchangeables.

De plus, la frugalité des données est souvent utilisée à tort pour parler de minimisation des données [BIE 20] ou de réduction des données [ESU 20]. Cependant, la minimisation de données est seulement une technique qui pourrait nous permettre d'atteindre la frugalité.

Encore, la frugalité des données comme présentée dans les travaux existants s'intéresse principalement au côté technique des processus de gestion de données. L'analyse de la conformité des données ou des objectifs de l'utilisation de la donnée avec les exigences des utilisateurs n'a pas été étudiée en rapport avec ces trois aspects. De plus, plusieurs techniques d'optimisation ou de minimisation de ressources existent à certaines phases du cycle de vie des données, mais souvent les conséquences de ces actions d'optimisation sur les autres phases du cycle de vie de la donnée ne sont pas analysées.

5.3. *Problématique*

Alors, ce travail de recherche s’articule autour de la problématique suivante : "Comment définir une gestion frugale de données ?" et "Comment mesurer et piloter le niveau de frugalité du processus de gestion de données ?".

Afin de répondre à cette problématique, nous allons présenter l'avancement de nos recherches qui peut être décliné à deux niveaux différents : (i) une définition exhaustive de la frugalité pour la gestion des données et la définition de son positionnement par rapport aux autres concepts "green", (ii) plusieurs futurs axes de recherche visant une gestion frugale de données.

5.4. *Actions réalisées*

Dans le contexte expliqué plus tôt, nous pouvons conclure que la frugalité n'a pas de définition concrète ni en data management ni en informatique de manière générale. Cependant, il est évident que

[8] https://global.toyota/en/company/vision-and-philosophy/production-system/

[9] https://www.cnil.fr/fr/reglement-europeen-protection-donnees

les acteurs économiques continuent à utiliser ce concept de manière plus extensive même si ils le font de façon erronée. Alors, notre objectif est de proposer une définition claire est exhaustive qui pourra être utilisée comme référence pour les futures recherches dans ce domaine.

La confusion entre *responsabilité environnementale*, *durabilité* et *frugalité* vient principalement des trois aspects communs auxquels ces concepts s'intéressent : l'aspect *Économique*, *Sociétal* et celui *Environnemental*.

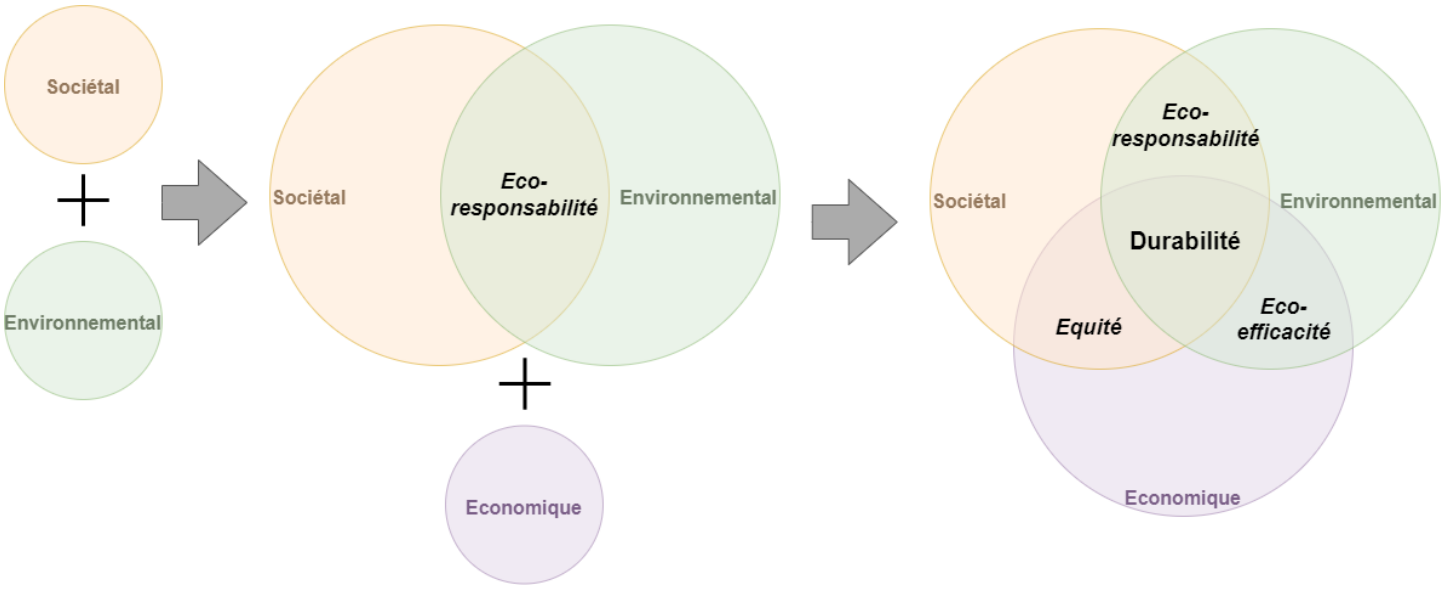

Figure 7. *Interdépendances entre l'éco-responsabilité et la durabilité*

Comme représenté dans la Figure 7, la convergence entre les aspects sociétal et environnemental aboutit au concept d'éco-responsabilité. En d'autres termes, l'éco-responsabilité s'intéresse à la diminution de l'impact écologique conformément aux réglementations environnementales, et aux mesures sociétales adoptées dans ce sens, comme la prévention et la sensibilisation.

Cependant, la croissance économique reste un objectif d'actualité, notamment dans un contexte tenant compte de l'environnement. Alors, la durabilité émerge comme résultat de la convergence des trois aspects, comme représenté sur la Figure 7. Cette conceptualisation de la durabilité est souvent retrouvé dans la littérature scientifique, mais elle n'a pas de point d'origine unique [PUR 19].

La durabilité, qui fait référence à la capacité d'une solution ou d'un processus à conserver ses caractéristiques spécifiques au fil du temps, assure l'efficience de l'activité économique en respect avec les aspects environnementales et sociétales.

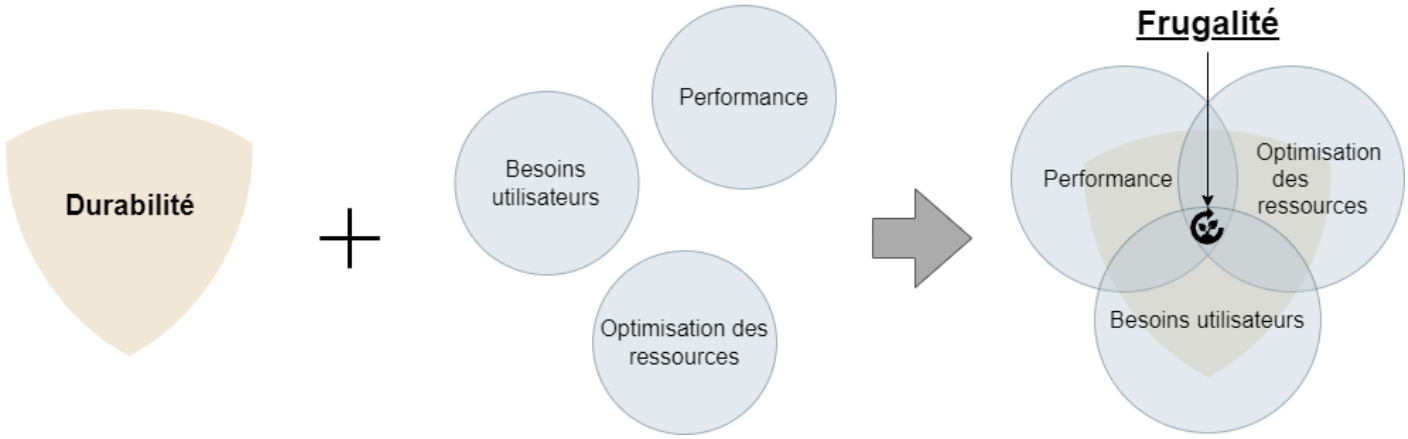

Figure 8. *Interdépendances entre la durabilité et la frugalité*

Comme présenté sur la Figure 8, nous définissons la frugalité en informatique comme une solution satisfaisant les principes de la durabilité tout en visant l'optimisation de ressources, la consolidation ou l'amélioration du niveau de qualité de service et la réponse aux besoins métier.

Nos premiers travaux nous ont permis également de proposer une définition complète de la frugalité du management de données.

Définition : La Gestion Frugale de Données est une approche de gestion de données qui consiste en l'utilisation des données de manière efficiente tout au long de leur cycle de vie (acquisition, stockage, traitement, dissémination et maintenance) en respect avec les normes techniques, juridiques et éthiques. L'efficience se traduit par le centrage de l'optimisation des ressources sur les exigences des utilisateurs dans un objectif de maintenance du niveau de qualité de service.

Pour clarifier les spécificités de cette définition, nous allons procéder à une analyse approfondie de ses éléments constitutifs.

– L'efficacité est définie comme le rapport entre les données utiles et les données totales entrées, souvent exprimée en pourcentage, et elle mesure dans quelle mesure un système, ou dans notre cas le processus de gestion des données, convertit les ressources d'entrée en données de sortie utiles en minimisant les pertes et en maximisant les performances.

– Dans le contexte de la gestion des données, la performance peut être définie comme la mesure de l'efficacité avec laquelle ce système atteint ses objectifs ou fonctions prévues.

– Afin de garantir que les données utilisées sont pertinentes, les évaluations de performance impliquent généralement de comparer les résultats réels à des normes, des références ou des objectifs prédéfinis pour déterminer l'efficacité du système dans différentes conditions. Pour respecter la centration sur l'utilisateur souhaitée par la frugalité dans la gestion des données, les normes, références et objectifs pris en compte pour l'évaluation de la frugalité doivent faire l'objet de discussions avec les différents types d'utilisateurs.

– Dans la gestion des données, la centration sur l'utilisateur consiste à concevoir et optimiser les systèmes de données pour répondre aux besoins spécifiques des utilisateurs. Cela implique de garantir que les données sont pertinentes, accessibles et faciles à utiliser, avec des décisions basées sur les retours et le comportement des utilisateurs pour améliorer leur expérience globale.

– La définition d'une « norme » englobe souvent divers aspects, y compris les dimensions techniques, juridiques, sociétales et éthiques. Une norme est un ensemble de règles, critères ou directives. Elle peut inclure des aspects techniques (formats de données, protocoles), juridiques (conformité aux lois et réglementations), sociétaux (protection des droits des utilisateurs) et éthiques (respect de la vie privée et de la transparence). Les normes servent de référence pour évaluer la performance et garantir que les systèmes respectent des exigences prédéfinies.

5.5. *Actions futures*

Nos premiers travaux sur la frugalité de la gestion de données nous ont permis de répondre à la première question de notre problématique au travers de la définition que nous avons proposée. Pour répondre en intégralité à notre problématique, nous avons identifié trois verrous technologiques :

1. Le premier obstacle vise à **qualifier** les données et les traitements associés selon deux axes : (i) réduction des données en fonction du besoin métier et (ii) minimisation des coûts et de l'impact environnemental. Nous souhaiterons proposer un système de métriques nous permettant d'évaluer le niveau de frugalité du processus de gestion de données mise en place. Notre objectif est de proposer un système d'évaluation multicritères ayant comme résultat un score global de frugalité. Les critères permettant ce calcul peuvent être formalisés par des éléments mesurant le niveau d'optimisation de ressources, le niveau de performance ou le niveau de cohérence entre la solution et le besoin utilisateur.

2. Le deuxième obstacle vise à définir une politique de frugalité **mesurable**, conforme aux exigences réglementaires et environnementales en vigueur, tout en optimisant l'utilisation des ressources disponibles et les exigences métier. La frugalité telle que nous l'avons définie, remet en question les architectures existantes, comme les lacs de données qui reposent sur les principes de stockage de la totalité des données brutes et des transformations associées. Nous envisageons de mesurer la frugalité selon plusieurs critères : le type de données, les architectures choisies, les environnements de stockage (on *cloud* ou on *premise*) et le niveau de satisfaction des besoins exprimés par les utilisateurs. Notre objectif est d'introduire une nouvelle technique de conception frugale ("frugality by design") qui permettrait d'intégrer les principes de frugalité dès les premières phases du développement des nouvelles solutions.

3. Le troisième obstacle consiste dans la mise en place d'un *pilotage* du management frugal de données, reposant sur un monitoring en temps réel des mesures de frugalité définies précédemment et sur des recommandations d'actions d'amélioration de la frugalité. L'objectif est de fournir une stratégie de pilotage générique et facilement configurable en fonction des besoins et des ressources.

5.6. *Conclusion*

Nos travaux de recherche se centrent sur la frugalité associée au management de données. Nos premiers travaux consistent en une analyse profonde de la littérature scientifique au sujet de la frugalité et des concepts associés qui nous a permis de définir les lacunes en matière de recherche.

La conclusion de cette première étape de notre recherche étant que nous avons observé un manque de compréhension de ce concept, notre première contribution se matérialise à travers d'une définition de la frugalité pour la gestion de données.

Nous avons présenté plusieurs axes de recherche : (i) qualification des données et traitements associés, (ii) mesure de la frugalité et (iii) pilotage d'un management frugal de données. La partie la plus cruciale de nos futurs travaux concerne la définition de métriques visant à établir un compromis équilibré entre les éléments des trois piliers – sociétal (comme le niveau de conformité aux exigences en matière de protection des données à caractère personnel), économique (par exemple, l'efficacité des coûts et des ressources) et environnemental (telle que l'empreinte carbone).

6. Conclusion[10]

Cet article propose une synthèse des travaux présentés lors du Forum JCJC de l'édition INFORSID 2024. Les contributions de quatre doctorants abordent des thématiques d'actualité qui illustrent l'engagement croissant de la communauté INFORSID en faveur de systèmes d'information responsables, intégrant un usage réfléchi de l'intelligence artificielle. Chaque partie s'attaque à des enjeux majeurs des SI, tels que la sécurité, l'éthique des publications scientifiques, l'utilisation raisonnée de l'IA ou encore la gestion sobre des données. Cette orientation vers des valeurs sociétales et environnementales — trop souvent négligée — est ici clairement affirmée, et mérite d'être poursuivie avec conviction.

Bibliographie

[ADA 19] adam. (2019, juillet 7). GDPR : Use only the data you need. Data + People. https://www.datapluspeople.com/gdpr-use-only-the-data-you-need/

[10] Mario CORTES CORNAX

[AGL 22] Aglietti V., Dhir N., Gonzalez J., Damoulas T., « Dynamic Causal Bayesian Optimization », NeuIPS 2021, 2021.

[AGR 23] Agrawal G., Pal K., Deng Y., Liu H., Baral C., « AISecKG: Knowledge Graph Dataset for Cybersecurity Education », *AAAI-MAKE 2023: Challenges Requiring the Combination of Machine Learning 2023*, 2023.

[ALL 23] Allison D., Smith P., McLaughlin K., « Digital Twin Enhanced Incident response for Cyber Physical Systems », Proceedings of the 18th International Conference on Availability, Reliability and Security, p. 1-10, 2023.

[ARM 19] M. F. e. a. Armstrong, « Reference errors in otolaryngology-head and neck surgery literature », Otolaryngology–head and neck surgery : official journal of American Academy of Otolaryngology-Head and Neck Surgery (2018)

[ASH 16] Ashangani, K., Wickramasinghe, K. U., De Silva, D. W. N., Gamwara, V. M., Nugaliyadde, A., & Mallawarachchi, Y. (2016, October). Semantic video search by automatic video annotation using TensorFlow. In 2016 Manufacturing & Industrial Engineering Symposium (MIES) (pp. 1-4). IEEE.

[ASL 20] Aslan O., A comprehensive review on malware detection approaches, IEEE Access, 2020.

[BIE 20] Biega, A. J., Potash, P., Daumé, H., Diaz, F., & Finck, M. (2020). Operationalizing the Legal Principle of Data Minimization for Personalization. Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval, 399-408. https://doi.org/10.1145/3397271.3401034

[BIR 08] S. Bird, R. Dale, B. Dorr, B. Gibson, M. Joseph, M.-Y. Kan, D. Lee, B. Powley, D. Radev, Y. Tan, « The acl anthology reference corpus: A reference dataset for bibliographic research in computational linguistics », 2008

[BOR 22] F. Bordignon, « Critical citations in knowledge construction and citation analysis: from paradox to definition », Scientometrics 127 (2022) 959–972.

[CAR 17] Carreira, Joao, and Andrew Zisserman. "Quo vadis, action recognition? a new model and the kinetics dataset." In proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 6299-6308. 2017.

[CHA 16] Chatras B., Softwarisation et Webification, la révolution logicielle des réseaux, De nouvelles architectures de communication, Paris, 2016.

[COP 23] Coppolino L., Nardone R., Petruolo A., Romano L., Souvent A., « Exploiting digital twin technology for cybersecurity in smart grids», Proceedings of the 18th International Conference on Availability, Reliability and Security, p. 1-10, 2023.

[DAR 22] Anonymous Authors., « Utilizing Graph Theory to derive multi-domain, risk prioritized attack paths within computer networks», DarkTrace AI Research, 2022.

[DAI 17] Dai, Angela, Angel X. Chang, Manolis Savva, Maciej Halber, Thomas Funkhouser, and Matthias Nießner. "Scannet: Richly-annotated 3d reconstructions of indoor scenes." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 5828-5839. 2017.

[DAS 21] Dasgupta S., Piplai A., Ranade P., Joshi A., « Cybersecurity Knowledge Graph Improvement with Graph Neural Networks », 2021 IEEE International Conference on Big Data (Big Data), 2021.

[DEF 16] Defferrard, Michaël, Xavier Bresson, and Pierre Vandergheynst. "Convolutional neural networks on graphs with fast localized spectral filtering." Advances in neural information processing systems 29 (2016).

[DEL 19] Devlin, Jacob, Ming-Wei Chang, Kenton Lee and Kristina Toutanova. “BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding.” North American Chapter of the Association for Computational Linguistics (2019).

[DEV 18] J. Devlin, M. Chang, K. Lee, K. Toutanova, « BERT: pre-training of deep bidirectional trans formers for language understanding », CoRR abs/1810.04805 (2018)

[DIE 20] Dietz M., Englbrecht L., Pernul G., « Enhancing industrial control system forensics using replication-based digital twins », Advances in Digital Forensics XVII, p. 21-38, 2021.

[ECK 19] Eckhart M., Ekerlhart A., « Digital twins for cyber-physical systems security: State of the art and outlook », Security and Quality in Cyber-Physical Systems Engineering, p. 383-412., 2029.

[EKT 23] Ektefaie, Yasha, George Dasoulas, Ayush Noori, Maha Farhat, and Marinka Zitnik. "Multimodal learning with graphs." Nature Machine Intelligence 5, no. 4 (2023): 340-350.

[EMP 22] Empl P., Schlette D., Zupfer D., Pernul G., « SOAR4IoT: Security IoT Assets with Digital Twins », Proceedings of the 17th International Conference on Availability, Reliability and Security, p. 1-10, 2022.

[ESU 20] Esubalew Aman Mezmir. (2020). Qualitative Data Analysis : An Overview of Data Reduction, Data Display and Interpretation. Research on Humanities and Social Sciences. https://doi.org/10.7176/RHSS/10-21-02

[FAR 16] Farid, M., Roatis, A., Ilyas, I. F., Hoffmann, H.-F., & Chu, X. (2016). CLAMS : Bringing Quality to Data Lakes. Proceedings of the 2016 International Conference on Management of Data, 2089-2092. https://doi.org/10.1145/2882903.2899391

[FIN 21] Finck, M., & Biega, A. J. (2021). Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems. Technology and Regulation, 44-61 Pages. https://doi.org/10.26116/TECHREG.2021.004

[FRA 23] François M., Arduin PE., Merad M., Classification of Decision Support Systems for Cybersecurity, 15th Mediterranean Conference on Information Systems (MCIS) and the 6th Middle East \& North Africa Conference on digital Information Systems (MENACIS), 2023.

[FRA 24a] François, M.; Arduin, P.-E.; Merad, M. « Physics-Informed Graph Neural Networks for Attack Path Prediction.» J. Cybersecur. Priv. 2025, 5, 15. https://doi.org/10.3390/jcp5020015

[FRA 24b] François M., Arduin PE., Merad M., « Latent States: model-based machine learning perspectives on cyber resilience », IEEE 4th Intelligent Cybersecurity Conference, 2024. https://doi.org/10.1109/ICSC63108.2024.10894907

[FRA 25] François M., Arduin PE., Merad M., « Enhancing Deep Learning Based IDS Adversarial Robustness With Causal Inference »,, 2025, IEEE 2025 5th International Conference on Cyber Security and Resilience (CSR). IEEE.

[GAS 18] Gasparini, Francesca, Ilaria Erba, Elisabetta Fersini and Silvia Corchs. “Multimodal Classification of Sexist Advertisements.” International Conference on E-Business and Telecommunication Networks (2018).

[GIL 17] Gilmer, Justin, Samuel S. Schoenholz, Patrick F. Riley, Oriol Vinyals, and George E. Dahl. "Neural message passing for quantum chemistry." In International conference on machine learning, pp. 1263-1272. PMLR, 2017.

[GLE 11] C. Glenton, B. Carlsen, « What about n? a methodological study of sample-size reporting in focus group studies », BMC Med Res Methodol (2011)

[GLE 19] C. Glenton, B. Carlsen, « When “normal” becomes normative: A case study of researchers’ quotation errors when referring to a focus group sample size study », International Journal of Qualitative Methods 18 (2019), 1609406919841251

[GOE 23] Goel D., Neumann A., Neumann F., Nguyen H., Guo M., « EVOLVING REINFORCEMENT LEARNING ENVIRONMENT TO MINIMIZE LEARNER’S ACHIEVABLE REWARD: AN APPLICATION ON HARDENING ACTIVE DIRECTORY SYSTEMS», arXiv Preprint, n° 2304.03998v1, 2024.

[HAN 89] J. A. Hanley, et al., « Receiver operating characteristic (roc) methodology: the state of the art », Crit Rev Diagn Imaging 29 (1989) 307–335[HOL 21] Holden J., Analyzing Open Shortest Path First (OSPF) Network with Neo4j and Cipher, 2021.

[HOM 23] Homaei M., Gutierrez OM., Nunez J., Vegas M., Lindo A., « A Review of Digital Twins and their Application in Cybersecurity based on Artificial Intelligence », arXiv preprint, n° 2311.01154, 2023.

[HON 23] Hong W., Yin J., You M., Wang H., Cao J., Li J., Liu M., Man C., « A graph empowered insider threat detection framework based on daily activities », ISA transactions, n° 141, p. 84-92, 2023.

[HUS 19] Hussain, Jabbar. "Deep learning black box problem." (2019).

[IAN 15] Iannacone M., Bohn S., Nakamura G., Gerth J., Huffer K., Bridges R., Ferragut E., Goodall J., « Developing and ontology for cyber security knowledge graphs », Proceedings of the 10th Annual Cyber and Information Security Research Conference, p. 1-4, 2023.

[JAC 21] Jacobs J., Romanosky S., Edwards B., Arjerid I., Roytman M., Exploit prediction scoring system (epss) », Digital Threats: Research and Practice, n° 3, p. 1-17., 2021.

[JEB 21] C. M. J. Jebari C, Herrera-Viedma E, « The use of citation context to detect the evolution of research topics: a large-scale analysis », Scientometrics (2021)

[JIA 18] Jiang, Yu-Gang, Zuxuan Wu, Jinhui Tang, Zechao Li, Xiangyang Xue, and Shih-Fu Chang. "Modeling multimodal clues in a hybrid deep learning framework for video classification." IEEE Transactions on Multimedia 20, no. 11 (2018): 3137-3147.

[JURGENS 18] D. Jurgens, S. Kumar, R. Hoover, D. McFarland, D. Jurafsky, « Measuring the Evolution of a Scientific Field through Citation Frames », Transactions of the Association for Computational Linguistics 6 (2018), 391–406

[KEV 22] CISA., Known Exploited Vulnerabilities, CISA GOV, 2022.

[KIM 13] Kim, J., Gwon, R. H., Park, J. T., Kim, H., & Kim, Y. S. (2013, December). A semi-automatic video annotation tool to generate ground truth for intelligent video surveillance systems. In Proceedings of International Conference on Advances in Mobile Computing & Multimedia (pp. 509-513).

[KRI 18] Krizinger W., Karner M., Traar G., Henjes J., Sihn W., « Digital Twin in manufacturing: A categorial literature review and classification », Ifac-PapersOnline, n° 11, p. 1016-1022, 2018.

[KUK 20] Kukleva, Anna, Makarand Tapaswi, and Ivan Laptev. "Learning interactions and relationships between movie characters." In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 9849-9858. 2020.

[LAC 85] G. De Lacey, C. Record, J. Wade, « How accurate are quotations and references in medical journals? », Br Med J (Clin Res Ed) 291 (1985), 884–886.

[LEC 98] LeCun, Yann, Léon Bottou, Yoshua Bengio, and Patrick Haffner. "Gradient-based learning applied to document recognition." Proceedings of the IEEE 86, no. 11 (1998): 2278-2324.

[LI 23] Li H., Shi Z., Pan C., Zhao D., Sun N., « Cybersecurity Knowledge Graphs Construction and Quality Assessment », Complex & Intelligent Systems, p. 1-17, 2023.

[LIA 18] Liang, Xiaodan, Ke Gong, Xiaohui Shen, and Liang Lin. "Look into person: Joint body parsing & pose estimation network and a new benchmark." IEEE transactions on pattern analysis and machine intelligence 41, no. 4 (2018): 871-885.

[LIU, CHEN 13] S. Liu, C. Chen, « The differences between latent topics in abstracts and citation contexts of citing papers », Journal of the American Society for Information Science and Technology 64 (2013), 627–639

[LIU 17] H. Liu, « Sentiment analysis of citations using word2vec », CoRR abs/1704.00177 (2017)

[LIU 19] Liu, Xinchen, Wu Liu, Meng Zhang, Jingwen Chen, Lianli Gao, Chenggang Yan, and Tao Mei. "Social relation recognition from videos via multi-scale spatial-temporal reasoning." In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 3566-3574. 2019.

[LIU 22] Liu K., Wang F., Ding Z., Liang S., Yu Z., Zhou Y., « A review of knowledge graph application scenarios in cyber security », arXiv preprint, n° 2204.04769, 2022.

[LOH 23] Lohn, A., Knack, A., Burke, A., Jackson, K. « Autonomous cyber defence: a roadmap from lab to ops. », Center for Emerging Technology and Security, 2023.

[LUH 20] Luh R., Temper M., Joa S., Schrittwieser S., Janicke H., « PenQuest: a gamified attacker/defender meta model for cybersecurity assessment and eduction », Journal of Computer Virology and Hacking Techniques, n°16, p. 16-61, 2020.

[MAR 10] Marr, David. Vision: A computational investigation into the human representation and processing of visual information. MIT press, 2010.

[MAR 19] Martinez J, Iglesias-Comesa C., Garcia-Nieto P., « Machine learning techniques applied to cybersecurity», International Journal of Machine Learning and Cybernetics, n° 10, p. 2823-2836, 2019.

[NAN 16] Nanda S., Predicting network attack patterns in SDN using machine learning approach, IEEE, Palo Alto, 2016.

[NAR 19] Nargesian, F., Zhu, E., Miller, R. J., Pu, K. Q., & Arocena, P. C. (2019). Data lake management : Challenges and opportunities. Proceedings of the VLDB Endowment, 12(12), 1986-1989. https://doi.org/10.14778/3352063.3352116

[NGO 23] Ngo HQ., Guo M., Nguyen H., « Near Optimal Strategies for Honeypots Placement in Dynamic and Large Active Directory Networks », AAMAS 2023, 2023.

[PAL 22] Paleyes A., Urma RG., Lawrence ND., « Challenges in deploying machine learning: a survey of case studies », ACM Computing Surveys, n° 6, p. 1-29., 2022.

[PEI 20] N. Peinelt, D. Nguyen, M. Liakata, « tBERT: Topic Models and BERT Joining Forces for Semantic Similarity Detection », Association for Computational Linguistics, Online, 2020

[PUR 19] Purvis, B., Mao, Y., & Robinson, D. (2019). Three pillars of sustainability : In search of conceptual origins. Sustainability Science, 14(3), 681-695. https://doi.org/10.1007/s11625-018-0627-5

[QOD 18] Qodseya, Mahmoud. "Managing heterogeneous cues in social contexts: A holistic approach for social interactions analysis." PhD diss., Université Paul Sabatier-Toulouse III, 2020.

[SAL 19] Salva S., Regainia L., « A catalog associating security patterns and attack steps to design secure applications », Journal of Computer Security, n°1, p. 49-74, 2019.

[SHA 18] Sharma R., Guliera A., Singla RK., « An overview of flow-based anomaly detection», International Journal of Communication Networks and Distributed Systems, n° 21, p. 220-240, 2018.

[SHA 20] Sharma, N., & Panwar, D. (2020). Green IoT : Advancements and Sustainability with Environment by 2050. 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 1127-1132. https://doi.org/10.1109/ICRITO48877.2020.9197796

[SHA 22] Shanmugam, D., Diaz, F., Shabanian, S., Finck, M., & Biega, A. (2022). Learning to Limit Data Collection via Scaling Laws : A Computational Interpretation for the Legal Principle of Data Minimization. Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency, 839-849. https://doi.org/10.1145/3531146.3533148

[SIV 20] Shailesh, S., & Judy, M. V. (2020). Automatic annotation of dance videos based on foot postures. Indian Journal of Computer Science And Engineering, Engg Journals Publications-ISSN, 976, 5166.

[SUB 19] Subroto A., Apriyana A., « Cyber risk prediction through social media big data analytics and statistical machine learning », Journal of Big Data, n°1, p. 50, 2019.

[SUH 23] Suhail S., Iqbal M., Hussain R., Jurdak R., « ENIGMA: an explainable digital twin security solution for cyber physical systems», Computers in Industry, n° 151, 2023.

[SYE 16] Syed Z., Padia A., Finin T., Mathews L., Joshi A., « UCO: A Unified cybersecurity ontology », UMBC Student Collection – AAAI Press, 2016.

[TAK 23] Takko T., Bhattacharya K., Lehto M., Jalasvirta P., Cederberg A., Kaski K., « Knowledge mining of unstructured information: application to cyber domain», Nature Scientific Reports, n°1, p. 1714, 2023.

[TE 22] S. Te, A. Barhoumi, M. Lentschat, F. Bordignon, C. Labbé, F. Portet, « Citation Context Clas sification: Critical vs Non-critical », Association for Computational Linguistics, Gyeongju, Republic of Korea, 2022

[TIS 15] Tisdale S., « Cybersecurity: Challenges from a Systems, Complexity, Knowledge Management and Business Intelligence Perspective », Issues on Information Systems, n° 3, 2015.

[TRACTIVE] Vers une analyse multimodale automatique de l'esthétique discursive filmique, https://anr.fr/Projet-ANR-21-CE38-0012,

[VAS 21] Vassilev V., Swinsky-Mydlarz V., Gasiorowsky P., Ouazzane K., Phipps A., « Intelligence graphs for threat intelligence and security policy validation of cyber systems », Proceedings of International Conference on Artificial Intelligence and Applications: ICAIA 2020, p. 125-139, 2021.

[VIC 17] N.J. Vickers, « Animal communication: When i'm calling you, will you answer too? », Current Biology 27 (2017) R713–R715

[VIC 18] Vicol, Paul, Makarand Tapaswi, Lluis Castrejon, and Sanja Fidler. "Moviegraphs: Towards understanding human-centric situations from videos." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 8581-8590. 2018.

[ZHA 20] Zhang K., Liu J., « Review on the application of knowledge graph in cyber security assessment », IOP Conference Series: Materials Science and Engineering, n° 5, 2020.

[ZHA 13] Zhang, L., Wu, C., Li, Z., Guo, C., Chen, M., & Lau, F. C. M. (2013). Moving Big Data to The Cloud : An Online Cost-Minimizing Approach. IEEE Journal on Selected Areas in Communications, 31(12), 2710-2721. IEEE Journal on Selected Areas in Communications. https://doi.org/10.1109/JSAC.2013.131211

