JULES MARTIAL YIN-BELTA MBARA

CURRICULUM VITÆ SCIENTIFIQUE — CANDIDATURE POSTDOCTORALE

Chicoutimi, Québec, Canada | 418 550-3151 | julesmartialmbara@gmail.com | LinkedIn

PROFIL SCIENTIFIQUE

Mon parcours académique s'est construit progressivement autour des réseaux, des télécommunications et de la cybersécurité. Après une licence en réseaux et télécommunications à l'Université de Bangui (2016–2019), j'ai poursuivi une maîtrise en informatique et technologie de l'information, concentration management, innovation et technologies des systèmes collaboratifs, à l'Université Polytechnique de Bucarest, en Roumanie, avec un mémoire consacré à la sécurisation du réseau sans fil. Je poursuis aujourd'hui un doctorat en informatique à l'Université du Québec à Chicoutimi (UQAC), où je suis membre de la Chaire de recherche institutionnelle sur la cyberdéfense et la protection des données personnelles (CYBPRO). Mes travaux doctoraux portent sur la cybersécurité industrielle et la conception d'architectures de confiance pour les jumeaux numériques industriels. J'étudie notamment l'intégrité vérifiable des données, l'interopérabilité sécurisée, la gouvernance distribuée, la résilience et l'auditabilité des décisions en mobilisant la blockchain, les technologies de registres distribués, IPFS, l'IoT/IIoT et les systèmes cyberphysiques. Mon parcours combine recherche expérimentale, projets financés en partenariat, évaluation de la cybersécurité d'organisations industrielles, publications évaluées par les pairs et enseignement universitaire en sécurité de l'IoT.

DOMAINES DE RECHERCHE

Cybersécurité industrielle · Jumeaux numériques industriels de confiance · IoT/IIoT et systèmes cyberphysiques · Blockchain et technologies de registres distribués (Hyperledger Fabric, Solana, Corda) · IPFS et stockage distribué · Interopérabilité industrielle sécurisée · Cyberrésilience · Gouvernance et auditabilité · IA et apprentissage fédéré appliqués à la cybersécurité.

FORMATION UNIVERSITAIRE

Doctorat en informatique — Université du Québec à Chicoutimi (UQAC)

- Automne 2023 – automne 2026 (soutenance de thèse)
- **Thèse —** *Decentralized Trust Architectures for Industrial Digital Twin Ecosystems*
- Direction : Prof. Fehmi Jaafar (UQAC) | Codirection : Prof. Pierre-Martin Tardif (Université de Sherbrooke)

Maîtrise en informatique et technologie de l'information — Université Polytechnique de Bucarest, Roumanie

- 2020 – 2023
- Concentration : Management, innovation et technologies des systèmes collaboratifs — 120 crédits ECTS
- **Mémoire —** *Système de sécurisation du réseau sans fil*

Licence en réseaux et télécommunications — Université de Bangui

- 2016 – 2019

EXPÉRIENCE DE RECHERCHE ET PROJETS FINANCÉS

Chercheur — volet cybersécurité et développement backend, projet Cogni-Actif

Université du Québec à Chicoutimi (UQAC), Québec, Canada — 15 décembre 2025 – 15 décembre 2026

Projet de recherche réalisé dans le cadre d'une bourse de recherche de 22 000 $ accordée pour mon implication au sein du projet Cogni-Actif. Le projet est financé par le ministère de l'Économie, de l'Innovation et de l'Énergie (MEIE), les Fonds SOVAR ainsi que l'entreprise Studio ExeCo.

- Responsable du volet cybersécurité : analyse et sécurisation de l'architecture du projet, notamment des composantes applicatives, des mécanismes d'authentification et de contrôle d'accès, des flux de données et des échanges entre les différents services.

- Identification des risques et vulnérabilités, définition d'exigences de sécurité et intégration des principes de sécurité dès la conception (Security by Design) dans l'évolution de la solution.
- Développement, restructuration et évolution du backend de la plateforme Cogni-Actif afin de faciliter l'intégration sécurisée des différents services et composantes du système et de préparer l'architecture aux versions évolutives du jeu; amélioration de la modularité et de la maintenabilité, intégration des interfaces de communication avec la plateforme du jeu, adaptation de l'architecture aux nouvelles fonctionnalités.
- Formulation et validation de mesures de protection visant la confidentialité, l'intégrité et la disponibilité des données; documentation des choix d'architecture et des mécanismes de sécurité en collaboration avec les partenaires du projet.

Expert stagiaire en cybersécurité — mandat Mitacs, ERAC Gaspésie
Québec, Canada — Octobre 2024 – mars 2025 (mandat de six mois)

Mandat de recherche appliquée en cybersécurité réalisé dans le cadre du programme Mitacs auprès de plusieurs entreprises partenaires de la région de la Gaspésie.

- Évaluation de la posture de cybersécurité des organisations accompagnées : analyse des politiques et pratiques de sécurité, identification des vulnérabilités et des écarts de protection, évaluation des mécanismes de sécurité déjà en place.
- Travaux portant sur les contrôles d'accès, les mécanismes d'authentification, la sécurité des infrastructures informatiques, la protection des données, la gestion des incidents et les pratiques organisationnelles de cybersécurité.
- Formulation de recommandations techniques et organisationnelles adaptées aux réalités des PME et élaboration de plans de réponse aux incidents visant à améliorer leur capacité de prévention, de détection et de réaction.
- Cette expérience de terrain a contribué à la dimension empirique de mes travaux de recherche sur les défis de cybersécurité et de confiance numérique rencontrés par les organisations industrielles évoluant dans des environnements disposant de ressources techniques et humaines limitées.

EXPÉRIENCE D'ENSEIGNEMENT UNIVERSITAIRE

Chargé de cours — 8INF917-11 : Sécurité informatique pour l'Internet des Objets
Université du Québec à Chicoutimi (UQAC), Chicoutimi, Québec — Trimestre d'hiver 2026, 45 heures

- Chargé de l'enseignement du cours universitaire 8INF917-11 — Sécurité informatique pour l'Internet des Objets, consacré aux problématiques de cybersécurité propres aux environnements IoT.
- Préparation et présentation des contenus pédagogiques : menaces et vulnérabilités des objets connectés, mécanismes d'authentification et de contrôle d'accès, sécurité des communications, protection des données et stratégies de sécurisation des architectures IoT.
- Conception des travaux, projets et évaluations, encadrement des étudiants et évaluation de leur capacité à analyser les risques, à identifier les vulnérabilités et à proposer des mécanismes de protection adaptés aux systèmes IoT.

CONTRIBUTIONS SCIENTIFIQUES DOCTORALES

C1 — Diagnostic empirique de la cybersécurité des PME industrielles
Évaluation de trente PME industrielles situées dans une région isolée de l'Est du Canada, au moyen de questionnaires, d'entretiens semi-structurés, d'évaluations techniques sur site et d'une analyse organisationnelle. Cette contribution met en évidence un déficit structurel de confiance numérique touchant notamment la segmentation réseau, les ports exposés, les pare-feu, les politiques de cybersécurité et l'obsolescence des infrastructures.

C2 — TwinIpfsChain : intégrité vérifiable en temps réel
Conception d'une architecture combinant un réseau Solana privé et IPFS pour assurer l'intégrité vérifiable des données de jumeaux numériques en temps réel. L'évaluation expérimentale rapporte une latence transactionnelle moyenne

d'environ 218 ms, un débit maximal mesuré de 26 457 transactions par seconde et la détection de tous les cas injectés de falsification de données, de manipulation d'empreintes cryptographiques et de rejeu.

C3 — SecDT : gestion sécurisée et décentralisée des jumeaux numériques industriels
Développement d'une architecture combinant Hyperledger Fabric 2.5, un déploiement IPFS privé à cinq nœuds, une gouvernance multi-organisationnelle permissionnée, des contrats intelligents, un stockage hors chaîne chiffré et des mécanismes de contrôle d'accès. Le prototype a été évalué sur quatorze machines virtuelles à partir des jeux de données NASA C-MAPSS FD001–FD004.

C4 — Interopérabilité industrielle interorganisationnelle décentralisée
Conception d'une architecture de partage de données entre organisations combinant Corda, IPFS et une couche d'intégration prenant en charge REST, MQTT, OPC UA et des systèmes hérités. L'environnement expérimental représente cinq organisations et étudie la provenance, l'autorisation, la traçabilité et la gouvernance distribuée au-delà de la simple compatibilité protocolaire.

C5 — Gouvernance décisionnelle auditable des jumeaux numériques
Développement d'un cadre combinant FA3ST/AAS, Hyperledger Fabric et IPFS afin de préserver une relation reconstructible entre l'état du jumeau numérique, le contexte de politique, le mode de décision, l'action, les preuves hors chaîne et l'engagement sur chaîne. L'approche distingue les modes autonome, humain dans la boucle et substitution manuelle, tout en séparant l'exécution locale à faible latence du chemin d'audit distribué.

APPROCHES MÉTHODOLOGIQUES ET EXPÉRIMENTALES

Conception de prototypes et de bancs d'essai distribués · déploiements multi-machines virtuelles · protocoles expérimentaux reproductibles · analyse de performance et de scalabilité · mesures de latence et de débit · scénarios de défaillance et de stress contrôlé · validation de l'intégrité, de la traçabilité, de la confidentialité et du contrôle d'accès · comparaison avec des architectures de référence centralisées ou distribuées.

FINANCEMENTS DE RECHERCHE

- **Bourse d'excellence — Département d'informatique et de mathématique (DIM), UQAC** 2 000 $ CAD, obtenue à deux reprises (2024 et 2026), pour un même montant de 2 000 $ CAD à chaque édition.
- **Bourse de recherche — Projet Cogni-Actif, UQAC** 22 000 $ CAD | 15 décembre 2025 – 15 décembre 2026. Financement : ministère de l'Économie, de l'Innovation et de l'Énergie (MEIE), Fonds SOVAR et Studio ExeCo.
- **Soutien financier de recherche — MITACS Accélération et CRSNG** 20 000 $ CAD | 1er août 2026 – 31 juillet 2027. Financement provenant d'une subvention Accélération MITACS et d'une subvention à la découverte du CRSNG, destiné à soutenir la poursuite des travaux doctoraux en cybersécurité et la mise en œuvre de méthodes de sécurisation des données fondées sur les chaînes de blocs.

PUBLICATIONS SCIENTIFIQUES

Articles de revue

- Mbara, Jules Martial Yin-Belta, Fehmi Jaafar et Pierre-Martin Tardif. *« SecDT: A Secure and Decentralized Approach for Industrial Digital Twins Using Blockchain and IPFS. »* IEEE Internet of Things Journal. IEEE, 2026. DOI : 10.1109/JIOT.2026.3704519
- Mbara, Jules Martial Yin-Belta, Fehmi Jaafar et Pierre-Martin Tardif. *« Auditable Decision Governance for Industrial Digital Twins Using Hyperledger Fabric and IPFS. »* IEEE Transactions on Industrial Informatics, 2026 (accepté pour publication).

Articles de conférences et d'ateliers

- Mbara, Jules Martial Yin-Belta, Fehmi Jaafar et Pierre-Martin Tardif. *« Cross-Organizational Data Governance for Industrial Digital Twins Using Blockchain and IPFS. »* Proceedings of the 8th International Workshop on Software Engineering Research and Practices for the IoT (SERP4IoT '26). ACM, 2026. DOI : 10.1145/3786159.3788474

- Mbara, Jules Martial Yin-Belta, Fehmi Jaafar et Pierre-Martin Tardif. *« A Decentralized Architecture for Industrial Data Interoperability Using Blockchain and IPFS. »* 2025 IEEE Conference on Dependable, Autonomic and Secure Computing (DASC). IEEE, 2025. DOI : 10.1109/DASC68382.2025.00013
- Mbara, Jules Martial Yin-Belta, Fehmi Jaafar et Pierre-Martin Tardif. *« TwinIpfsChain: Ensuring Decentralized Data Integrity in Real-Time Digital Twins for Industry 5.0 Using Blockchain and IPFS. »* 2025 7th International Conference on Blockchain Computing and Applications (BCCA). IEEE, 2025. DOI : 10.1109/BCCA66705.2025.11229546
- Mbara, Jules Martial Yin-Belta, Fehmi Jaafar et Pierre-Martin Tardif. *« Security Evaluation of Industrial Organisations in an Isolated Region. »* 2025 11th International Conference on Control, Decision and Information Technologies (CoDIT). IEEE, 2025. DOI : 10.1109/CoDIT66093.2025.11321624

Autre publication évaluée par les pairs

- Pierre, Tom, Jules Martial Yin-Belta Mbara et Fehmi Jaafar. *« Solana–IPFS Architecture for Scalable, Low-Cost, and Secure Digital Identity Management in Real Estate Transactions. »* IEEE Access, vol. 14, pp. 99094–99111, 2026. DOI : 10.1109/ACCESS.2026.3706191

EXPÉRIENCE TECHNIQUE ANTÉRIEURE SÉLECTIONNÉE

- Administration de systèmes et d'infrastructures réseau, gestion des comptes et des mises à jour, sauvegardes, sécurité des postes de travail et résolution d'incidents techniques.
- Installation et maintenance d'équipements réseau, administration de pare-feu et serveurs, sauvegardes, mécanismes de sécurité et soutien aux utilisateurs.

COMPÉTENCES SCIENTIFIQUES ET TECHNIQUES

- **Cybersécurité industrielle et systèmes critiques —** analyse de risques et de vulnérabilités; intégrité, confidentialité et contrôle d'accès; détection de falsification et de rejeu; résilience; réponse aux incidents; sécurité des systèmes cyberphysiques et des environnements IoT/IIoT.
- **Blockchain et confiance distribuée —** Hyperledger Fabric 2.5, Solana, Corda, contrats intelligents, gouvernance permissionnée, ancrage cryptographique, provenance, traçabilité et auditabilité.
- **Jumeaux numériques et stockage distribué —** Industrial Digital Twins, FA3ST/AAS, IPFS, stockage adressé par contenu, preuves hors chaîne, gestion d'états et reconstruction d'historiques.
- **Interopérabilité et protocoles —** MQTT, OPC UA, REST, TCP/IP, CoAP/DTLS, BLE; intégration de systèmes industriels hétérogènes et de systèmes hérités.
- **Programmation, données et expérimentation —** Python, Java, C++, JavaScript/TypeScript, Node.js, FastAPI, MySQL, PostgreSQL; déploiements distribués, machines virtuelles, benchmarking, analyse de latence et de débit, tests de défaillance et scénarios de stress contrôlé.

AFFILIATIONS SCIENTIFIQUES

- IEEE — Student Member
- Membre de la Chaire de recherche institutionnelle sur la cyberdéfense et la protection des données personnelles (CYBPRO), Université du Québec à Chicoutimi

PERSONNES DE RÉFÉRENCE

Prof. Fehmi Jaafar

- Professeur agrégé, Département d'informatique et de mathématique, Université du Québec à Chicoutimi (UQAC) — Titulaire de la Chaire de recherche institutionnelle sur la Cyberdéfense et la protection des données personnelles (CybPro)
- Directeur de thèse
- Téléphone : 418 545-5011, poste 2606 | Courriel : fjaafar@uqac.ca

Prof. Pierre-Martin Tardif

- Professeur agrégé, Département des systèmes d'information et méthodes quantitatives de gestion, École de gestion, Université de Sherbrooke — Chercheur associé au Centre de recherche interdisciplinaire en cybersécurité de l'UdeS (CRICUS)
- Codirecteur de thèse
- Courriel : Pierre-Martin.Tardif@USherbrooke.ca

LANGUES

Français : langue maternelle | Sango : langue nationale | Anglais : intermédiaire-avancé | Roumain : intermédiaire

TRAVAIL ACADÉMIQUE COMPLÉMENTAIRE

- *« Security Vulnerabilities in Artificial Intelligence Systems »* — travail académique réalisé sous la supervision du Prof. Fehmi Jaafar (UQAC) et du Prof. Pierre-Martin Tardif (Université de Sherbrooke).