الجمهورية الشعبية الديمقراطية الجزائرية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للإعلام الآلي 08 ماي 1945
École Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbès

THESIS

To obtain the diploma of **State engineer**
Field: **Computer Science**
Specialty: **Ingénierie des Systèmes Informatiques (ISI)**

Theme

Secure and Decentralized Approach for Collaborative Learning in ICPS

Presented by:
Maria TAKHI
Submission Date: **Sept, 2024**
In front of the jury composed of:

Mr. Abdelhamid MALKI	President
Ms. Sidi Mohammed BENSLIMANE	Co-Supervisor
Ms. Samir OUCHANI	Supervisor
Mr. Fayssal BENDAOUD	Examiner

Academic Year : 2023/2024

Abstract

Federated Learning (FL) is a decentralized machine learning paradigm that enables the training of models across distributed devices, maintaining data privacy and minimizing communication overhead. However, FL's reliance on a central server introduces critical vulnerabilities, such as a Single Point of Failure attack (SPoF) and increased susceptibility to Distributed Denial of Service attacks (DDoS) attacks. To mitigate these challenges, the integration of blockchain technology with Federated Learning, referred to as Blockchain-based Federated Learning (BCFL), has emerged as a robust solution. BCFL enhances system security by incentivizing participant contributions, deterring malicious behavior, and eliminating the dependency on a central server. This approach is particularly promising in domains such as the Industrial Internet of Things (IIoT), healthcare, telemedicine, and cyber-physical systems, where data security and reliability are paramount. In this graduation project, we will provide an in-depth analysis of ML techniques within the context of Industrial ndustrial Cyber-Physical Systems (ICPS), with a particular focus on Federated Learning. We will also explore blockchain technology, highlighting cutting-edge solutions that address the integration of blockchain with FL. Following this theoretical foundation, we will present our novel framework, FedChain-IPFS, which leverages both FL and blockchain technologies. To validate the effectiveness of our approach, we conducted extensive experiments, benchmarking the performance of FedChain-IPFS against traditional FL environments using two distinct aggregation algorithms: FedGA and FedPer. The results of these tests will demonstrate the superiority of our solution in terms of security, scalability, and efficiency.

Keywords— Federated Learning, Blockchain, Smart contract, Cyber-physical systems, IPFS

الملخص

يُعد التعلم الفيدرالي (FL) نموذجًا لا مركزيًا للتعلم الآلي يتيح تدريب النماذج عبر أجهزة موزعة، مع الحفاظ على خصوصية البيانات وتقليل تكاليف الاتصال. ومع ذلك، فإن اعتماد التعلم الفيدرالي على خادم مركزي يقدم نقاط ضعف حرجة، مثل نقطة الفشل الواحدة (Single Point of Failure, SPoF) وزيادة الحساسية لهجمات حجب الخدمة الموزعة (DDoS). لمعالجة هذه التحديات، ظهرت تقنية الدمج بين التعلم الفيدرالي وتقنية البلوكشين، والمعروفة بالتعلم الفيدرالي القائم على البلوكشين (BCFL) كحل قوي. يعمل هذا النموذج على تعزيز أمان النظام من خلال تحفيز مساهمات المشاركين، وردع الأنشطة الخبيثة، وإزالة الاعتماد على الخادم المركزي. تُعد هذه المقاربة واعدة بشكل خاص في مجالات مثل إنترنت الأشياء الصناعي (IIoT)، الرعاية الصحية، الطب عن بعد، والأنظمة السيبرانية الفيزيائية، حيث تكون أمان البيانات والموثوقية ذات أهمية بالغة. في هذا المشروع التخرجي، سنقدم تحليلًا متعمقًا لتقنيات التعلم الآلي في سياق الأنظمة السيبرانية الفيزيائية الصناعية (ICPS)، مع التركيز بشكل خاص على التعلم الفيدرالي. كما سنستعرض تقنية البلوكشين، مع تسليط الضوء على الحلول المتطورة التي تتناول دمج البلوكشين مع التعلم الفيدرالي. بعد تقديم الأسس النظرية، سنقدم إطار عملنا المبتكر FedChain-IPFS، الذي يستفيد من تقنيات التعلم الفيدرالي والبلوكشين معًا. لإثبات فعالية نهجنا، قمنا بإجراء تجارب مكثفة، حيث قمنا بمقارنة أداء FedChain-IPFS مع البيئات التقليدية للتعلم الفيدرالي باستخدام خوارزميتين مختلفتين للتجميع: FedGA و FedPer. ستظهر نتائج هذه التجارب تفوق حلنا من حيث الأمان، القابلية للتوسع، والكفاءة.

الكلمات المفتاحية: البلوكشين، التعلم الفيدرالي، الأنظمة السيبرانية الفيزيائية، IPFS.

Résumé

L'Apprentissage Fédéré (FL) est un paradigme d'apprentissage automatique décentralisé qui permet l'entraînement de modèles sur des appareils distribués, tout en préservant la confidentialité des données et en réduisant les coûts de communication. Cependant, la dépendance du FL à un serveur central introduit des vulnérabilités critiques, telles qu'un point de défaillance unique (Single Point of Failure, SPoF) et une sensibilité accrue aux attaques par déni de service distribué (DDoS). Pour atténuer ces défis, l'intégration de la technologie blockchain avec l'Apprentissage Fédéré, appelée Apprentissage Fédéré basé sur la Blockchain (BCFL), s'est révélée être une solution robuste. Le BCFL renforce la sécurité du système en incitant les contributions des participants, en dissuadant les comportements malveillants, et en éliminant la dépendance à un serveur central. Cette approche est particulièrement prometteuse dans des domaines tels que l'Internet Industriel des Objets (IIoT), la santé, la télémédecine, et les systèmes cyber-physiques, où la sécurité des données et la fiabilité sont primordiales. Dans ce projet de fin d'études, nous fournirons une analyse approfondie des techniques d'apprentissage automatique dans le contexte des systèmes cyber-physiques industriels (ICPS), en mettant l'accent sur l'Apprentissage Fédéré. Nous explorerons également la technologie blockchain, en soulignant les solutions de pointe qui abordent l'intégration de la blockchain avec le FL. Après cette base théorique, nous présenterons notre cadre novateur, FedChain-IPFS, qui exploite à la fois les technologies FL et blockchain. Pour valider l'efficacité de notre approche, nous avons mené des expériences approfondies, en comparant les performances de FedChain-IPFS à celles des environnements FL traditionnels, en utilisant deux algorithmes d'agrégation distincts : FedGA et FedPer. Les résultats de ces tests démontreront la supériorité de notre solution en termes de sécurité, de scalabilité et d'efficacité.

Mots-clés: Apprentissage Fédéré, Blockchain, Contrat Intelligent, Systèmes Cyber-Physiques, IPFS.
