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 **Master**
Field: **Computer Science**
Specialty: **Ingénierie des Systèmes Informatiques (ISI)**

Theme

Blockchain-based Federated Learning approaches: A State-of-the-Art

---

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

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

Academic Year : 2023/2024

Abstract

Federated Learning (FL) is a decentralized machine learning approach that enables models to be trained across multiple devices, thereby preserving data privacy and reducing communication costs. However, FL's dependence on a central server introduces vulnerabilities such as Single Point of Failure (SPoF) and susceptibility to Distributed Denial of Service (DDoS) attacks. Integrating blockchain technology with federated learning, known as Blockchain-Based Federated Learning (BCFL), has emerged as a promising solution to address these deficiencies. BCFL incentivizes participant contributions and deters malicious activities, showing significant potential in applications like the Industrial Internet of Things, healthcare, telemedicine, and cyber-physical systems. This work provides a comprehensive overview of FL and blockchain technologies, delves into the architecture of BCFL, proposes a classification for BCFL approaches, and reviews existing approaches dealing with these challenges. A comparative analysis is presented, and future research directions are highlighted to enhance the reliability and effectiveness of model training in BCFL.

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

الملخص

التعلم الفيدرالي (FL) هو نهج لامركزي للتعلم الآلي يتيح تدريب النماذج عبر عدة أجهزة، مما يحافظ على خصوصية البيانات ويقلل من تكاليف الاتصال. ومع ذلك، فإن اعتماد FL على خادم مركزي يقدم ثغرات مثل نقطة الفشل الوحيدة (SPoF) والقابلية للهجمات عبر نفي الخدمة الموزع (DDoS). وقد ظهرت تقنية البلوكشين كمزيج مع التعلم الفيدرالي، المعروف باسم التعلم الفيدرالي المبني على البلوكشين (BCFL)، ككل واعد للتعامل مع هذه العيوب. يُحفز BCFL مساهمات المشاركين ويمنع الأنشطة الضارة، ويظهر إمكانات كبيرة في تطبيقات مثل الإنترنت الصناعي للأشياء، والرعاية الصحية، والتطبيب عن بُعد، والأنظمة السيبرانية الفيزيائية. يقدم هذا العمل نظرة شاملة على تقنيات FL والبلوكشين، ويتناول بنية BCFL، ويقترح تصنيفًا لأساليب BCFL، ويستعرض الأساليب الحالية التي تتعامل مع هذه التحديات. تُقدَّم مقارنة تحليلية، ويتم تسليط الضوء على اتجاهات البحث المستقبلية لتعزيز موثوقية وفعالية تدريب النماذج في BCFL.

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

Résumé

L'apprentissage fédéré (FL) est une approche décentralisée de l'apprentissage automatique qui permet de former des modèles sur plusieurs dispositifs, préservant ainsi la confidentialité des données et réduisant les coûts de communication. Cependant, la dépendance du FL à un serveur central introduit des vulnérabilités telles que le Point Unique de Défaillance (SPoF) et la susceptibilité aux attaques par Déni de Service Distribué (DDoS). L'intégration de la technologie blockchain avec l'apprentissage fédéré, connue sous le nom d'Apprentissage Fédéré Basé sur la Blockchain (BCFL), s'est révélée être une solution prometteuse pour remédier à ces défauts. Le BCFL incite les contributions des participants et décourage les activités malveillantes, montrant un potentiel significatif dans des applications telles que l'Internet Industriel des Objets, les soins de santé, la télémédecine et les systèmes cyber-physiques. Ce travail propose une vue d'ensemble complète des technologies FL et blockchain, explore l'architecture du BCFL, propose une classification des approches BCFL et examine les approches existantes traitant de ces défis. Une analyse comparative est présentée, et les orientations futures de la recherche sont soulignées pour améliorer la fiabilité et l'efficacité de l'entraînement des modèles dans le BCFL.

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