

Improving The OPENFL Mechanism to Avoid Federated Learning Poisoning Attacks in Blockchain Networks

Nouh Suhel Abboud^{*} 

Dr. Hiba Haider^{**}

(Received 5 / 5 / 2026. Accepted 14 / 7 / 2026)

□ ABSTRACT □

The integration of federated learning with blockchains represents a promising paradigm for collaborative artificial intelligence systems that preserve privacy. However, these decentralized environments are vulnerable to poisoning attacks, where malicious participants can sabotage the final model by sending malicious updates. This research paper proposes an enhanced mechanism to counter Random Noise Attack within blockchain-based federated learning environments. The enhanced mechanism is based on the OPENFL mechanism architecture, with an improvement to the method of making the voting decision inside it, by replacing the evaluation based on model accuracy and validation data with cosine similarity that measures the alignment of weight directions. We compared the proposed mechanism with the original OPENFL based on validation data, FEDCHALLENGER which uses cosine similarity, and FEDRDF which relies on Fast Fourier Transform, based on several metrics: efficiency, time cost, and GAS COST. Our experiments, conducted on a local Ethereum network using the Ganache simulator, the MNIST dataset, and a Convolutional Neural Network model, showed that the enhanced mechanism-maintained efficiency and improved time cost by 62.9% compared to the original OPENFL without causing an increase in cost (GAS) on the Ethereum network.

Keywords: Blockchain, Federated Learning, Poisoning Attacks.

Copyright  :Latakia University journal (formerly Tishreen) -Syria, The authors retain the copyright under a CC BY-NC-SA 04

^{*} Master's Student, Department of Computer System and Networks, Faculty of Information Engineering, Latakia University (formerly Tishreen), Latakia, Syria. noohabboud@gmail.com

^{**} Assistant Professor, Faculty of Information Engineering, Department of Computer System and Networks, Latakia University (formerly Tishreen), Latakia, Syria. hibaameen.haider@gmail.com

تحسين آلية OPENFL لتجنب هجمات تسميم التعلم الموحد في شبكات سلاسل الكتل

نوح سهيل عبود*

د. هبة حيدر**

(تاريخ الإيداع 5 / 5 / 2026. قُبِلَ للنشر في 14 / 7 / 2026)

□ ملخص □

يمثل دمج التعلم الموحد مع سلاسل الكتل نموذجاً واعداً لأنظمة الذكاء الاصطناعي التعاونية التي تحافظ على الخصوصية. مع ذلك، فإن هذه البيانات اللامركزية عرضة لهجمات التسميم، حيث يمكن للمشاركين الخبيثين تخريب النموذج النهائي من خلال إرسال تحديثات خبيثة. تقترح هذه الورقة البحثية آلية محسنة لمواجهة هجمات Random Noise Attack ضمن بيانات التعلم الموحد المعتمدة على سلاسل الكتل. تعتمد الآلية المُحسَّنة على بنية آلية OPENFL مع تحسين طريقة اتخاذ قرار التصويت داخلها، وذلك باستبدال التقييم المعتمد على دقة النموذج وبيانات التحقق بتشابه جيب التمام الذي يقيس توافق اتجاهات الأوزان. قارنا الآلية المقترحة مع OPENFL الأصلية المعتمدة على بيانات التحقق وFEDCHALLENGER التي تستخدم تشابه جيب التمام وFEDRDF التي تستخدم تحويل فورييه السريع وذلك اعتماداً على عدة مقاييس هي الكفاءة والتكلفة الزمنية وGAS COST. أظهرت تجاربنا التي أجريناها على شبكة Ethereum محلية باستخدام محاكي ganache ومجموعة بيانات MNIST ونموذج الشبكة العصبية الالتفافية (CNN)، أن الآلية المُحسَّنة حافظت على الكفاءة وحسّنت التكلفة الزمنية بنسبة 62.9% مقارنةً بالآلية OPENFL الأصلية دون أن تتسبب بزيادة في التكلفة (GAS) على شبكة Ethereum.

الكلمات المفتاحية: سلاسل الكتل، التعلم الموحد، هجمات التسميم.



حقوق النشر : مجلة جامعة اللاذقية (تشرين سابقاً) - سورية، يحتفظ المؤلفون بحقوق النشر

بموجب الترخيص CC BY-NC-SA 04

* طالب ماجستير، قسم النظم والشبكات الحاسوبية، كلية الهندسة المعلوماتية، جامعة اللاذقية (تشرين سابقاً)، اللاذقية، سورية.

noohabboud@gmail.com

**مدرس، قسم النظم والشبكات الحاسوبية، كلية الهندسة المعلوماتية، جامعة اللاذقية (تشرين سابقاً)، اللاذقية، سورية.

hibaameen.haider@gmail.com

1. مقدمة:

يُمكن التعلم الموحد من تدريب النماذج الجماعية دون الحاجة إلى مشاركة البيانات، وبالتالي الحفاظ على السرية المطلوبة في قطاعات حساسة مثل الرعاية الصحية والأنظمة المالية [1]. في الوقت نفسه، تُقدّم تقنية سلاسل الكتل حلاً مبتكراً لمشاكل الثقة والشفافية والأمان والاعتماد على خادم مركزي لأنظمة التعلم الموحد وذلك من خلال تسجيل المعاملات بشكل غير قابل للتغيير وإدارة العمليات عبر عقود ذكية قابلة للبرمجة [2]. إن الطبيعة المفتوحة لسلاسل الكتل العامة، تُعرض هذه الأنظمة الهجينة لمخاطر أمنية جسيمة منها هجمات Random Noise Attack التي تُصنف ضمن فئة Model Poisoning Attacks، وفيها تُشارك عقد خبيثة عمداً تحديثات مُشوّهة للنموذج بهدف تخريب النموذج العالمي النهائي [3]. يُشكّل هذا التهديد تحدياً جوهرياً لجدوى وفعالية التعلم الموحد في شبكات سلاسل الكتل، إذ أن غياب آليات دفاع قوية قد يُحوّل هذه الأنظمة الواعدة إلى أرض خصبة للأنشطة الخبيثة.

لمعالجة هذا التحدي، ظهرت عدة آليات لتجنب هجمات الضوضاء العشوائية، تهدف إلى التمييز بين المشاركين النزيهين والمخادعين، من أحدث هذه الآليات آلية OPENFL [4] والتي تعتبر آلية متكاملة تجمع بين الأمان والتحفيز، إذ تعتمد على عملية تصويت لامركزية يستخدم فيها المشاركون بيانات التحقق الخاصة بهم ليختبروا نماذج المشاركين الآخرين ويعتمدوا على عتبات معينة ليقوموا بالتصويت.

إن الاعتماد على العتبات التقليدية في OPENFL قد يسبب ظمناً لبعض المشاركين الذين قد تكون بيانات التدريب لديهم قليلة مقارنة بالآخرين مما قد يجعل نماذجهم ضعيفة عند مقارنتها بالعتبات ويتسبب بظلمهم في عملية التصنيف. إضافة إلى ذلك أشار الباحثون إلى أن مشكلات قابلية التوسع المحتملة تشكل تحدياً على OPENFL [4] وقد ينعكس ذلك على الزمن اللازم لتنفيذها. ركز الباحثون أيضاً على تقييم OPENFL من حيث قدرتها على تجنب المشاركين الخبيثين وتكلفتها المالية [4] إلا أنهم أهملوا جانباً بالغ الأهمية وهو التكلفة الزمنية التي تجبينا على السؤال التالي: ما هو الثمن (من حيث الوقت) الذي سيدفعه المشارك مقابل حصوله على نموذج آمن بطريقة لامركزية. انطلاقاً من هذه التحديات طرحنا مساهمة تحسينية لهذه الآلية في محاولة لتجاوز قيود العتبات لبيانات التحقق وتقليل التكلفة الزمنية دون التأثير على كفاءة هذه الآلية أو زيادة تكلفتها المالية. اعتمد تحسيننا على استبدال بيانات التحقق بتشابه جيب التمام مستبدلين إلى نقاط القوة التي يتمتع بها تشابه جيب التمام في تعامله مع المتجهات وحساب تشابهها.

2. أهمية البحث وأهدافه:

تتبع أهمية هذا البحث من الحاجة لتطوير آليات فعالة لاختيار العقد في أنظمة التعلم الموحد في شبكات سلاسل الكتل خاصة في ظل تزايد هجمات التسميم.

بالرغم من وجود آليات متعددة لتحديد المشاركين الخبيثين، فإن جزءاً كبيراً منها يعتمد على أساليب تحقق صارمة أو اختبارات تفرض تكلفة زمنية أو مالية عالية على النظام وتحد من قابلية التطبيق العملي لهذه الآليات عند التوسع لاسيما في الأنظمة الحساسة للوقت.

يهدف هذا البحث إلى معالجة هذه المشكلة من خلال تقديم آلية محسنة تعتمد تشابه جيب التمام الذي يقلل الوقت دون التأثير على جودة اختيار المشاركين أو التكلفة وهو ما يجعله خياراً عملياً وقابلًا للتطبيق في البيئات التي تتطلب استجابة سريعة دون التضحية بالأمان أو زيادة التكلفة المالية.

3. طرائق البحث ومواده:

اعتمدت هذه الدراسة على منهجية بحث تجمع بين الدراسة النظرية والتنفيذ العملي من خلال المحاكاة. تتضمن منهجية البحث الخطوات الآتية:

- دراسة المفاهيم النظرية المتعلقة بالتعلم الموحد وشبكات سلاسل الكتل وهجمات التسميم ودراسة آلية OPENFL.
- تحليل الدراسات السابقة التي تناولت هجمات تسميم التعلم الموحد وآليات مقاومتها.
- تصميم بيئة محاكاة تعتمد على محاكي GANACHE ومحرر VISUAL STUDIO CODE ولغة PYTHON لتنفيذ OPENFL وتحسينها.
- تقييم أداء آلية OPENFL المحسنة مع الآلية الأصلية وآلية FEDCHALLENGER وآلية FEDRDF.
- تحليل النتائج ومقارنتها لتحديد الفائدة من تحسين آلية OPENFL.

الدراسات المرجعية:

تعددت الدراسات المرجعية التي تناولت هجمات التسميم في التعلم الموحد بسبب مخاطرها العالية وضرورة إيجاد آليات لمقاومتها أو التخفيف من تأثيرها.

وضح الباحثون في [5] أن غياب آليات التحفيز الفعالة لتشجيع المشاركة، والاعتماد على خادم مركزي الذي يخلق نقطة فشل واحدة هي من أبرز التحديات التي تواجه التعلم الموحد وقد أشاروا إلى أن تقنية سلاسل الكتل تمتلك خصائص فريدة مثل اللامركزية والثبات وإمكانية التتبع، مما يجعلها مرشحاً مثالياً لمعالجة هذه التحديات. ومن أبرز ما قدمه الباحثون في [5] تصنيف نماذج أنظمة BLOCKFED إلى ثلاث فئات رئيسية بناءً على أدوار العقد في النظام، حيث تمثلت هذه الفئات في: النموذج المنفصل (Decoupled Model) الذي تعمل فيه العقد إما في التعلم الموحد أو سلاسل الكتل بشكل منفصل، والنموذج المزدوج (Coupled Model) الذي تؤدي فيه جميع العقد وظيفتي التعلم الموحد وسلاسل الكتل معاً، والنموذج المتداخل (Overlapped Model) الذي يمثل مزيجاً بين النموذجين السابقين. واعتبر الباحثون أن هذا التصنيف يُشكل إطاراً قيماً لفهم التنوع في تصميم أنظمة BLOCKFED حيث قدمت لنا هذه الدراسة تحليلاً لفهم كيفية عمل التعلم الموحد في شبكات سلاسل الكتل.

قدم الباحثون في [6] نظاماً للرعاية الصحية الذكية يدمج بين التعلم الموحد (Federated Learning) وسلاسل الكتل (Blockchain) في بيئة إنترنت الأشياء الطبي. يعتمد النظام على لجنة تحقق عشوائية تطبق خوارزمية Multi-KRUM لاستبعاد التدرجات الناتجة عن هجمات التسميم، إلا أن هذه الخوارزمية كانت تفترض معرفة مسبقة بعدد الأجهزة المهاجمة مما يضعف من كفاءة هذه الآلية في السيناريوهات الواقعية. اقترح الباحثون في [7] إطاراً يجمع اختبار الوسيط Median-based Testing مع خوارزمية Krum لزيادة فعالية كشف هجمات التسميم إلا أنهم اعتمدوا على افتراض أن معظم المشاركين هم مشاركون جيدين. اعتمد الباحثون في [8] آلية FLTRUST لمقاومة هجمات التسميم. تتطلب هذه الآلية إنشاء مصدر ثقة مركزي من خلال مجموعة بيانات جذرية نظيفة (Root Dataset) يتم استخدامها لتقييم موثوقية تحديثات العملاء اعتماداً على Cosine

Similarity ومنحها درجات ثقة قبل عملية التجميع. وقد أظهرت النتائج التجريبية تفوق FLTRUST على عدد من الآليات التقليدية مثل Krum و Trimmed Mean و Median. إلا أن هذه الآلية تتطلب توافر مجموعة بيانات جذرية نظيفة وممثلة للتوزيع الحقيقي للبيانات، وهو ما قد يكون صعب التحقيق في بعض البيانات العملية. كما أن أي انحراف في توزيع هذه البيانات قد يؤدي إلى تراجع فعالية آلية الثقة واتخاذ قرارات تجميع غير دقيقة، مما قد يتسبب في فشل الآلية.

قدم الباحثون في [9] آلية FoolsGold للدفاع ضد هجمات Sybil في التعلم الموحد، وتعتمد الآلية على قياس تشابه أوزان النماذج بين المشاركين باستخدام تشابه جيب التمام (Cosine Similarity)، انطلاقاً من فرضية أن العملاء الخبيثين المتعاونين ينتجون تحديثات أكثر تشابهاً من العملاء السليمين. وعند اكتشاف تشابه مرتفع بصورة غير طبيعية، تقوم الآلية بخفض معدل التعلم للمشاركين المشتبه بهم بدلاً من استبعادهم مباشرة، دون الحاجة إلى معرفة مسبقة بعدد المهاجمين. وقد أثبتت نتائج الدراسة فعاليتها في مواجهة هجمات Sybil، إلا أن تصميمها يستهدف العملاء الخبيثين المتعاونين بشكل أساسي.

وضح الباحثون في [10] أن آلية FEDRDF التي تعتمد على اختبار Kolmogorov-Smirnov(k-s) وتحويل فورييه السريع FFT لتحليل ارتباط الأوزان وكثافتها تتفوق على كل من الوسيط median والمتوسط المقطوع Trimmed Mean و Krum و FLTRUST عند وجود مهاجمين.

استخدم الباحثون في [11] آلية FEDCHALLENGER والتي تعتمد على طبقة تحدي-استجابة (challenge-response) هدفها الكشف المبكر عن احتمالية وجود مشاركين خبيثين ومن ثم طبقة تجميع قوية تهدف إلى حماية نموذج التعلم الموحد من التحديثات الخبيثة القادمة من العملاء الخبيثين عن طريق تحليل أوزان نماذج المشاركين باستخدام مقياسين رئيسيين هما Cosine Similarity و Median Absolute Deviation (MAD). وضح الباحثون قدرة هذه الآلية على تجنب المشاركين الخبيثين حتى بوجود 40% من المشاركين كمشاركين خبيثين إضافة إلى تفوقها على آليات حديثة مثل Krum و Trimmed Mean و DUEL.

قدم الباحثون في [4] آلية OPENFL التي تعد من أحدث آليات كشف العقد الخبيثة والتي لا تتطلب تسجيلاً مسبقاً أو قوائم بيضاء، إذ يُسمح لأي مستخدم على شبكة Ethereum بالمشاركة دون أي عوائق أو موافقات مسبقة. علاوة على ذلك، تعتمد OPENFL على نظام سمعة مدعوم بضمانات مالية، حيث ترتبط السمعة برهن مالي حقيقي. هذا الربط الاقتصادي يجعل الهجمات مكلفة ويمنع العقد الخبيثة من تبديل سلوكها بسهولة، لأن العقد تُخاطر بفقدان أموالها المودعة. تستخدم OPENFL طريقة تصويت مُرجحة بالسمعة، حيث تُرجح قوة التصويت بناءً على درجة السمعة العالمية (GRS) لكل مشارك. هذا يعني أن أصوات المشاركين الموثوق بهم لها تأثير أكبر على تقييم الآخرين، مما يزيد من دقة عملية الكشف ويُصعب على العقد الخبيثة التأثير على النتائج. توفر OPENFL آلية متكاملة تكافئ المشاركين الملتزمين برفع مستوى سمعتهم العالمية ومنحهم جزءاً من مكافآت الجولة والعقوبات المصادرة من الجهات الخبيثة وتعاقب المخالفين بخضم جزء من سمعتهم. لا تعتمد OPENFL على تخزين الأوزان على سلسلة الكتل والتي قد تتسبب بزيادة التكاليف وبدلاً من ذلك، تحتفظ OPENFL بمعظم البيانات خارج سلسلة الكتل، وتخزن فقط تجزئة الأوزان وبيانات التحقق الأساسية عليها، مما يقلل تكاليف الغاز ويجعل الآلية أكثر فعالية. انطلاقاً من هذه الميزات التي قدمتها OPENFL قمنا باختيارها ودرسناها ساعين إلى تقديم مساهمة تحسينية عليها.

يتضح من استعراض الدراسات السابقة أن الآليات المقترحة للدفاع ضد هجمات التسميم في التعلم الموحد تختلف في الفرضيات التي تعتمد عليها وفي طبيعة الهجمات التي تستهدفها، مما يجعل اختيار آليات للمقارنة ضمن دراستنا مسألة ترتبط بمدى توافق الآلية مع أهداف الدراسة والبيئة التشغيلية المعتمدة لدينا. تم اختيار الآليات المرجعية المستخدمة في هذه الدراسة وفق مجموعة من المعايير التي تضمن عدالة المقارنة وملاءمتها لسيناريو التجارب، كما هو موضح في الجدول (1) مع تنفيذ هذه الآليات ضمن البيئة التشغيلية نفسها.

الجدول 1 معايير اختيار الآليات

الآلية	قرار الدراسة	السبب
OPENFL الأصلية	أستخدمت	الأساس الذي بنيت عليه الآلية المقترحة، مما يسمح بتقييم أثر التحسين بصورة مباشرة.
Krum / Multi-Krum	لم تستخدم	تتطلب معرفة مسبقة بعدد المشاركين الخبيثين، وهو افتراض لا يتوافق مع بيئة دراستنا.
FLTrust	لم تستخدم	تعتمد على مجموعة بيانات مرجعية نظيفة وممثلة للتوزيع الحقيقي للبيانات وهذا لا يتوافق مع هدف دراستنا في التخلص من بيانات التحقق.
FoolsGold	لم تستخدم	تعتمد على تشابه جيب التمام وتحليل أوزان النماذج، إلا أنها صُممت للكشف عن هجمات Sybil الناتجة عن عملاء متعاونين، بينما تعتمد هذه الدراسة على هجوم Random Noise attack يُنفذ بشكل غير تعاوني.
FEDRDF	أستخدمت	تعتمد على تحليل خصائص أوزان النماذج، وتم تقييمها في مواجهة هجمات Model Poisoning، مما يجعلها متوافقة مع بيئة الدراسة.
FEDCHALLENGER	أستخدمت	تعتمد على تشابه جيب التمام لتحليل توافق أوزان النماذج، كما تم تقييمها في مواجهة هجمات Model Poisoning، مما يجعلها متوافقة مع بيئة الدراسة.

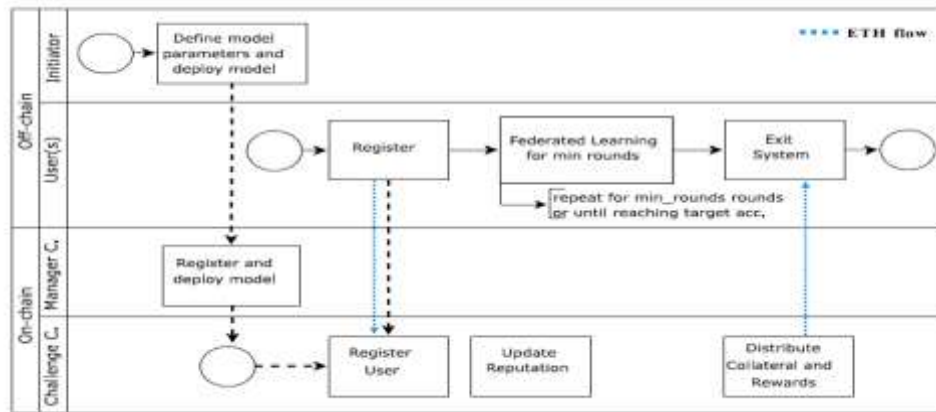
الأساسيات النظرية:

آلية OPENFL المحسنة:

تعتمد آليتنا على بنية OPENFL مع تحسين على عملية التقييم لاتخاذ قرار التصويت لنتم باستخدام تشابه جيب التمام Cosine Similarity بدلاً من بيانات التحقق.

مراحل عمل آلية OPENFL المحسنة:

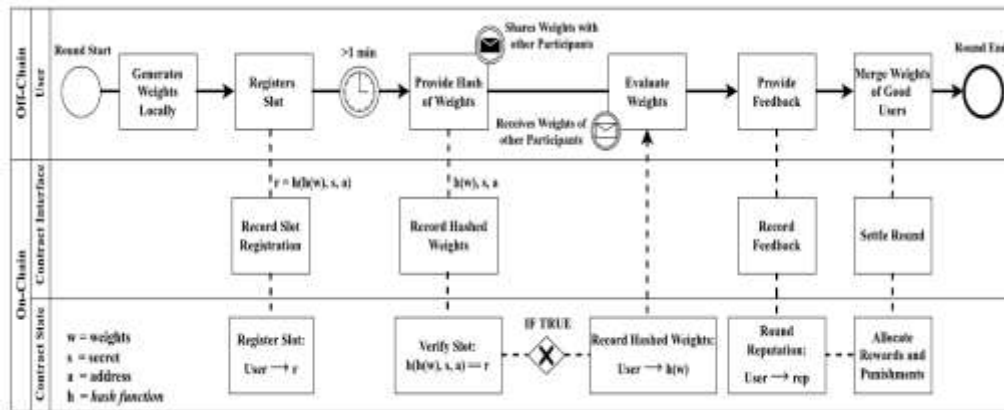
يمثل الشكل 1 العمليات الأساسية لآلية OPENFL المحسنة والتي تتم على شبكة سلاسل الكتل وخارجها بشكل مترابط.



الشكل 1 مراحل عمل آلية OPENFL [4].

1. يبدأ أحد المستخدمين (المُبادر – initiator) عملية إنشاء تحدٍ جديد للتعلم الموحد عن طريق تعريف بارامترات النموذج مثل بنية الشبكة العصبية وتعيين المتغيرات الأساسية مثل المكافأة والحد الأدنى والأقصى للضمان وعدد جولات التعلم ومُعامل العقاب [4].
2. يقوم المُبادر بإرسال معاملة إلى العقد الذكي manager تتضمن المعلومات والمتغيرات السابقة ويتم تسجيل هذا المُبادر تلقائياً كأول مشارك في النظام عبر العقد الذكي challenger [4].
3. انضمام المشاركين الآخرين: يمكن لأي مستخدم آخر على شبكة Ethereum الآن الانضمام إلى التحدي عن طريق تفاعله مع عقد التحدي challenger حيث يجب على كل مشارك جديد إيداع ضمان collateral وإرساله إلى عقد التحدي الذي يتحقق من أن هذا الضمان يقع ضمن الحد الأدنى والأعلى للضمان المطلوب للمشاركة [4].
4. يتم تهيئة درجة السمعة العالمية GRS – Global Reputation Score لكل مشارك بقيمة الضمان الذي أودعه وكذلك يتم تهيئة درجة سمعة الجولة Round Reputation Score – RRS لكل مشارك بالقيمة صفر [4]. GRS سيتم استخدامها كوزن للصوت الذي سيُصوت به المشارك لجعل أصوات المشاركين الجيدين أعلى تأثيراً من أصوات المشاركين الخبيثين على النتيجة النهائية للتصويت، و RRS تمثل التصنيف (جيد – خبيث) الذي حصل عليه المشارك خلال هذه الجولة بعد حساب مجموع الأصوات الموزونة التي حصل عليها خلال هذه الجولة [4].
5. بعد الانتهاء من عملية التسجيل والتهيئة يصبح المشاركون جاهزون لتنفيذ جولات التعلم الموحد حيث أنه في كل جولة يتم تنفيذ مجموعة من العمليات التي يتم من خلالها تحديد المشاركين الجيدين والخبيثين لتجميع نماذج الجيدين ويتم أيضاً تطبيق نظام مكافأة وعقوبة لتشجيع المشاركين الجيدين ومعاقبة الخبيثين [4].
6. بعد الانتهاء من تنفيذ جولات التعلم الموحد يمكن للمشاركين الخروج من النظام وكذلك فإن أي مشارك تنخفض سمعته العالمية أقل من حد معين سيتم إزالته تلقائياً من النظام. هذا الحد يُحسب بقسمة الحد الأدنى للضمان المطلوب على معامل العقاب (عندها لا يكون للمشارك أي أهمية في النظام) [4].

جولة التعلم الموحد في آلية OPENFL المحسنة:



الشكل 2 وصف جولة FL في نظام OPENFL [4].

يمثل الشكل 2 العمليات التي تتم خلال كل جولة تعلم موحد في آلية OPENFL المحسنة.

1. Round start: تبدأ جولة التعلم الموحد بعد انتهاء عملية التسجيل أو الجولة السابقة [4].
2. Generates Weights Locally: يقوم كل مشارك بتدريب نموذج المحلي باستخدام بياناته الخاصة ولعدد محدد من الدورات المحلية ويقوم بإنشاء hash لأوزانه. يبدأ الجميع بنفس بنية النموذج التي تم تحديدها من قبل المُبادر (initiator). تتم هذه العملية محلياً على المشارك خارج السلسلة (chain-off) [4].
3. Register slot: يقوم كل مشارك بنشر سر secret يحتوي على الهاش الخاص بأوزانه + قيمة عشوائية + عنوانه على السلسلة ليقوم العقد الذكي بتسجيل هذا secret. الهدف من secret هو ضمان أنه لم يتم أحد المشاركين بنسخ أوزان مشاركين آخرين أو ما يُعرف بهجوم السبق وكذلك لضمان أن المشارك لم يتم بتعديل أوزانه قبل تبادلها مع المشاركين الآخرين [4].
4. Waiting: ينتظر المشاركون لفترة زمنية معينة ليتم تسجيل secret الخاص بكل مشارك [4].
5. Provide Hash Weight: بعد انتهاء فترة الانتظار وقبل تبادل الأوزان يطلب العقد الذكي من المشاركين كشف الهاش الخاص بالأوزان والقيمة العشوائية ويقوم العقد الذكي بحساب secret والتحقق من تطابقها مع secret المقدمة خلال Register slot، وفي حال التطابق يتم تسجيل هاش الأوزان على سلسلة الكتل [4].
6. Off-chain Exchange: تمت محاكاة عملية تبادل النماذج عن طريق تخزين النماذج في مصفوفة وكل مشارك يحصل على نماذج الآخرين من هذه المصفوفة [4]. في الواقع يمكن أن يتبادل المشاركون النماذج فيما بينهم عبر قنوات أمانة خارج السلسلة (مثل IPFS) مما يقلل من التكلفة والحمل على الشبكة [4].
7. Verify Integrity: يتأكد كل مشارك من أن الأوزان التي تلقاها من الآخرين تطابق البصمات المسجلة على السلسلة وذلك بإعادة حساب البصمة ومقارنتها مما يمنع المشاركين من تقديم أوزان مختلفة عما التزموا به [4].
8. Evaluate weights: في OPENFL يقيم كل مشارك أداء نماذج الآخرين باستخدام مجموعة التحقق الخاصة به ليقوم بالتصويت إما ب 1 إذا كانت دقة المشارك الأخر أكبر من دقة نموذج أو أقل منها حتى 7% أو يصوت ب -1 عدا ذلك [4]، سنقوم بتحسين ذلك عن طريق جعل المشارك يقوم فقط بحساب تشابه

أوزانه مع أوزان المشاركين الآخرين عن طريق تشابه جيب التمام Cosine Similarity ليقوم بالتصويت بناءً على التشابه، حيث أن أوزان المشاركين الجيدين سيكون لها اتجاه متوافق (نحو التحسين) على عكس أوزان المشاركين السيئين والتي سيكون اتجاهها بعكس أوزان أو تحديثات المشاركين الجيدين. يُعتبر تشابه جيب التمام أحد المقاييس الأكثر شيوعاً وفعالية لحساب درجة التشابه بين المتجهات [11][12]. ويُعرف رياضياً بأنه حاصل قسمة الضرب الداخلي للمتجهين P و Q على حاصل ضرب طولي هذين المتجهين وذلك وفق المعادلة 1 [11][12]:

$$\text{Sim}_{\cos}(P, Q) = \frac{\langle P, Q \rangle}{\|P\| \|Q\|} \quad (1)$$

يكمن الأساس النظري المتين لهذه المعادلة في متباينة Cauchy-Schwarz inequality، والتي تضمن أن قيمة هذا التشابه تنحصر رياضياً في النطاق $[-1, 1]$ ، مما يجعله مطابقاً لسلوك دالة جيب التمام المثلثية [12]. من الناحية الهندسية، لا يهتم هذا المقياس بحجم المتجهات أو مقدارها (Magnitude)، بل يركز فقط على الزاوية بينها؛ وبالتالي فهو يقيس درجة التوافق في الاتجاه داخل فضاء المتجهات. إن هذه الخاصية الجوهرية، تمنح المقياس ميزة حاسمة عند مقارنة النماذج، لأنها تعني أن التشابه يُقاس بناءً على "نمط" أو "شكل" التمثيل الداخلي للنموذجين [11][12].

يُفسّر ناتج هذا التشابه بناءً على قيمته العددية حيث تشير القيمة 1 إلى أن متجهي النموذجين متطابقين تماماً في الاتجاه (أي أن الزاوية بينهما 0 درجة)، مما يعكس أقصى درجات التشابه. أما القيمة 0 فتعني أن المتجهان متعامدان (أي أن الزاوية بينهما 90 درجة)، مما يشير إلى عدم وجود تشابه جوهري بين النموذجين. في المقابل، تعكس القيمة -1 حالة التضاد التام، حيث يكون المتجهين في اتجاهين متعاكسين تماماً (الزاوية 180 درجة)، وهو ما يُفسّر على أنه نموذجان يمثلان أنماطاً متعاكسة أو متناقضة [11][12]. من الجدير بالذكر أنه في العديد من التطبيقات العملية، خاصة عندما تكون مكونات المتجهات غير سالبة (فيما يُعرف بالفضاءات الموجبة)، فإن نطاق القيم يقتصر على $[0, 1]$ مما يبسط التفسير حيث تقترب القيمة من الواحد كلما زاد التشابه [12]. بناءً على ذلك يقوم المشارك بالتصويت ب 1 للمشاركين الآخرين إذا كانت قيمة تشابه نمودجه مع نماذجهم قريبة من 1 (أكبر من 0.5) وفيما عدا ذلك يصوت ب -1. اعتمدت هذه الدراسة القيمة (0.5) كعتبة لاتخاذ قرار التصويت الإيجابي أو السلبي حيث يمكن لنماذج محلية ذات مستويات أداء أو دقة مختلفة أن تحقق قيمة مرتفعة لتشابه جيب التمام، طالما أن أوزانها تتجه نحو الهدف نفسه وتسهم في تحسين النموذج العالمي وقد استُرشد في اختيار هذه القيمة بالملاحظات الواردة في دراسة FEDCHALLENGER [11]، وذلك لكونها من الآليات التي تتوافق مع البيئة التشغيلية لهذه الدراسة كما وضعنا سابقاً وقد أظهرت نتائجها أن قيم تشابه جيب التمام الخاصة بالتحديثات السليمة أو المشاركين الجيدين تتركز عند قيم تتجاوز (0.7)، في حين تتركز قيم تشابه جيب التمام الخاصة بالتحديثات الخبيثة عند قيم أقل من (0.3)، مما يشير إلى وجود منطقة فاصلة بين التحديثات السليمة والخبيثة بدلاً من وجود قيمة حدية وحيدة. وانطلاقاً من هذه الملاحظة، تم اختبار عدة قيم للعتبة تقع داخل وبالقرب من هذه المنطقة الفاصلة أثناء التجارب الأولية للآلية المقترحة، شملت هذه القيم (0.5، 0.7، 0.8)، وكانت جميعها ملائمة ضمن بيئة وإعدادات التجارب المستخدمة في دراستنا، حيث وفرت تمييزاً عملياً بين أوزان النماذج المتوافقة

وغير المتوافقة. وبناءً على ذلك، تم اعتماد القيمة (0.5) لأنها تقع داخل المنطقة الفاصلة ولأنها تمثل أقل قيمة من القيم المختبرة حافظت على كفاءة التمييز بين التحديثات السليمة والخبيثة كما أنها تمنح الآلية قدرة أكبر على استيعاب الاختلافات في اتجاهات الأوزان. وتجدر الإشارة إلى أن اختيار هذه القيمة يعتمد على خصائص بيئة التعلم كطبيعة البيانات وتوزيعها لدى المشاركين، وبنية النموذج، وإعدادات التدريب، ولا يُعد قيمة معيارية ثابتة يمكن تعميمها على جميع سيناريوهات التعلم الموحد. ولذلك فإن القيمة 0.5 لا تمثل عتبة معيارية عامة وإنما تمثل اختياراً مناسباً لبيئة الدراسة الحالية.

قد يتأثر أداء تشابه جيب التمام عندما يصبح عدد المشاركين الخبيثين أكبر أو يساوي عدد الجيدين إلا أن الباحثون في [4] وضحو أن نظام المكافأة والعقوبة في OPENFL يفرض على المشارك دفع رهان كبير لكي يتمكن من الانضمام وبالنسبة للمشاركين الجيدين لن يكون لديهم أي مشكلة بذلك كونهم سيستردون رصيدهم ويحصلون على مكافآت عالية على عكس المشاركين الخبيثين الذي سيكونون متخوفين من دفع هذا الرهان الكبير مما يقلل من احتمالية مشاركة عدد كبير من المشاركين الخبيثين مما يعطي نقطة قوة إضافية لتشابه جيب التمام.

9. Submit Feedback: يرسل كل مشارك تقييماً (الأصوات) إلى العقد الذكي ليقوم بجمع الأصوات وحساب سمعة الجولة لكل مشارك بعد أن يتم وزن كل صوت بدرجة السمعة العالمية للمشارك الذي صوّته مما يعطي ثقة أكبر لأصوات المشاركين ذوي السمعة العالية [4].

10. Merge weights of good users: يختار العقد الذكي أحد المشاركين الجيدين ليقوم بتجميع أوزان المشاركين الذين تم تصنيفهم كمشاركين جيدين باستخدام خوارزمية المتوسط الموحد FEDAVG [4].

11. Settle and close round: يقوم العقد الذكي بحساب المكافآت (مكافأة + أموال صادرة من الخبيثين) والعقوبات بناءً على RRS وتنتقل هذه المكافأة أو العقوبة إلى السمعة العالمية GRS لكل مشارك، ويتم إعادة ضبط جميع متغيرات الجولة لتبدأ جولة جديدة [4].

12. تتكرر هذه المراحل في كل دورة حتى يصل النموذج إلى مستوى الأداء المطلوب أو حتى ينتهي العدد المحدد مسبقاً من الجولات أو عندما يتوقف تحسين النموذج (عندما يصبح الفرق بين النموذج الحالي والنموذج السابق ثابت لا يتحسن) [4].

نمط الهجوم:

في بحثنا نركز على هجوم Random Noise Attack الذي يصنف ضمن فئة هجمات تسميم النموذج Model Poisoning Attacks والتي تتميز بقدرتها على التأثير المباشر في أوزان النموذج المحلي للعميل أو بمعنى آخر يمكن القول أن gradient poisoning هو الأسلوب التنفيذي ل model poisoning [3]. بعكس هجمات تسميم النموذج فإن هجمات تسميم البيانات Data Poisoning Attacks تعمل بصورة غير مباشرة عبر تخريب بيانات التدريب أو تعديل تسمياتها [3] وتعتبر هجمات تسميم النموذج أكثر ضرراً من هجمات تسميم البيانات [3].

تعتمد طريقة عمل هذا الهجوم على قيام العميل الخبيث بإضافة قيم عشوائية (Random Noise) إلى أوزان نموذج العميل قبل إرسالها، بهدف التأثير سلباً في النموذج العالمي [3] بالتالي فهو مبني على الأوزان الأصلية مما يُصعب اكتشافه ويعتبر هذا الهجوم من الهجمات غير الموجهة (Untargeted Poisoning Attacks)، لأن الهدف منه هو تدهور أداء النموذج المجمع في جميع المهام، وليس التأثير في مهمة محددة [3] بالتالي يسبب ضرر كبير رغم بساطته.

يمكن أن يُطبق هذا الهجوم بشكل تعاوني منسق حيث يتعاون المشاركون الخبيثون مع بعضهم لزيادة الضرر وهو ما يعرف بهجمات التواطؤ collusion attacks أو يتم تنفيذه بشكل فردي غير منسق حيث يكون كل مشارك خبيث مستقل في عمله عن الآخر [3] وفي بحثنا اعتمدنا الهجوم بشكل فردي غير منسق.

4. النتائج والمناقشة:

توصيف بيئة العمل:

استخدمنا محاكي Ganache الذي يوفر لنا إمكانية تشغيل شبكة Ethereum محلية. يُقدّم المحاكي 10 حسابات بما في ذلك عناوينها ومفاتيحها الخاصة ومعاملاتها وأرصعتها (كل حساب 100 ETH افتراضي) مع إمكانية نشر العقود الذكية المبرمجة بلغة solidity عليه باستخدام أداة REMIX. اعتمدنا قاعدة بيانات MNIST في بحثنا حيث تُستخدم بشكل شائع في مجال التعلم الموحد وهي قاعدة بيانات خاصة بالتعرف على الأرقام المكتوبة بخط اليد وتحتوي صور لأرقام (0.....9) مكتوبة بخط اليد بتنسيق الأبيض والأسود وتضم 60000 صورة لأغراض التدريب و 10000 لأغراض الاختبار كل صورة بحجم 28 x 28 بيكسل [4]. قمنا بتوزيع هذه DATASET على المشاركين توزيع متجانس Independent and Identically Distributed بحيث يحصل جميع المشاركين على بيانات متشابهة إحصائياً وتحتوي على نفس الفئات أو بمعنى آخر أن جميع المشاركين لديهم جميع فئات البيانات (9...0) [4].

قمنا ببرمجة مهام التعلم الموحد وتوزيعها على الحسابات والتفاعل مع Ganache باستخدام لغة PYTHON ومكاتبها مثل WEB3 عبر محرر الأكواد visual studio code. قارنا OPENFL و OPENFL المحسنة و FEDCHALLENGER و FEDRDF انطلاقاً من بارامترات التهيئة التي يوضحها الجدول (2) مع مراعاة أن العقود الذكية لا تتعامل مع ETH مباشرة وإنما يجب تحويلها إلى وحدة WEI حيث أن $1\text{ETH} = 10^{18}\text{WEI}$.

الجدول 2 بارامترات المحاكاة

البارامتر	القيمة
عدد المشاركين الكلي	10
نسبة المشاركين الخبيثين	17% - 20% - 30% - 40%
المكافأة (REWARD)	$10^{18} = 1\text{ETH}$
عدد جولات التعلم الموحد	8
الحد الأدنى للرهان	$10^{18} = 1\text{ETH}$
الحد الأعلى للرهان	$1.8 * 10^{18} = 1.8\text{ETH}$
عدد جولات التدريب داخل المشارك EPOCHES	1
حجم دفعة البيانات BATCH_SIZE	32
عامل العقوبة PUNISHFACTOR	1/3 (خصم بمقدار ثلث الرصيد)
الجولة التي يغير بها المشارك سلوكه لخبيث	3

اعتمدنا على ثلاث مقاييس هي الكفاءة المتمثلة بدقة النموذج الناتج، التكلفة الزمنية، Gas Costs وفيما يلي توضيح لهذه المقاييس:

1-Accuracy: تمثل الدقة نسبة التنبؤات الصحيحة إلى إجمالي التنبؤات عند اختبار النموذج الناتج على بيانات اختبارية، ويتم التعبير عنها كنسبة مئوية، وفقاً للعلاقة التالية:

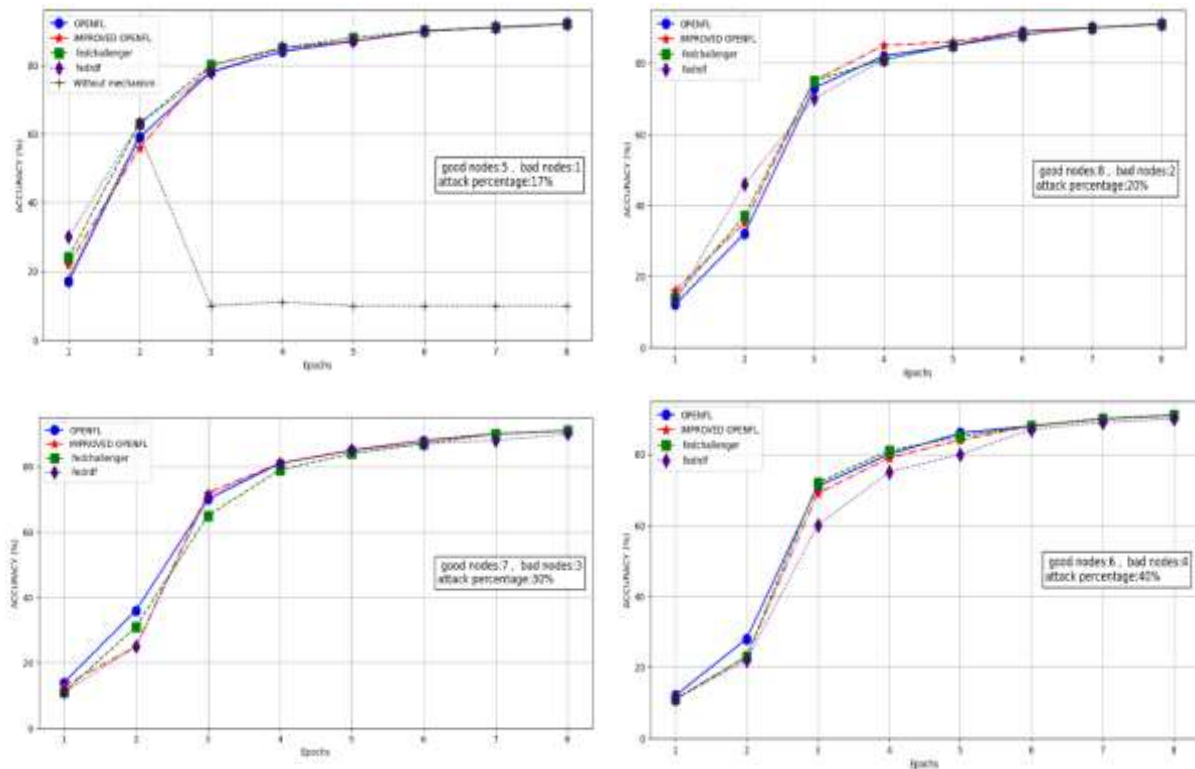
$$\text{Accuracy} = \text{number of correct predictions} / \text{total number of prediction} \quad (2)$$

2-time: يعبر عن مقدار الوقت الذي يستغرقه تنفيذ آلية تجنب هجمات التسميم أثناء التفاعل مع البلوكشين بدون زمن التدريب المحلي على المشاركين خلال جولة واحدة، يقدر هذا الوقت بالثواني.

3-Gas Costs: تكلفة الجولة التي يقوم بها المشارك على شبكة Ethereum، حيث أن كل عملية أو تابع يُنفذه المشارك على شبكة Ethereum يتطلب مقدار معين من الغاز (GAS) الذي يُقاس بوحدة GWEI وذلك حسب تعقيده. يتم حساب التكلفة عن طريق ضرب كمية الغاز أو GWEI المستهلكة بسعر ال GWEI والذي هو (20 GWEI لكل وحدة غاز [4] مع ملاحظة أن هذا السعر في الواقع يختلف من وقت لآخر حسب وضع الشبكة وإزدحامها، وهنا استخدمنا السعر الذي اعتمد عليه الباحثون في الدراسة [4] لكي نتمكن من الاستشهاد بالنتائج التي حصلوا عليها في هذه الدراسة عندما نقوم بالمقارنة. بعد ذلك يتم تحويل هذا المقدار إلى ETH لكي يدفعها المشارك كرسوم تنفيذ على Ethereum مع الأخذ بعين الاعتبار أن $1\text{ETH} = 10^9 \text{GWEI}$.

يُعتبر حساب التكلفة أمر ضروري في شبكات البلوكشين حيث يعتبر مقياساً أساسياً لمعرفة ما إذا كان استخدام آلية ما عملياً من الناحية المالية في العالم الحقيقي. إن تكاليف الغاز المرتفعة قد تجعل الآلية غير قابلة للتطبيق إذا كانت تفوق فوائد المشاركة.

السيناريو الأول: تقييم أداء آليات تجنب هجمات التسميم من حيث الكفاءة عند نسب مختلفة من الهجوم



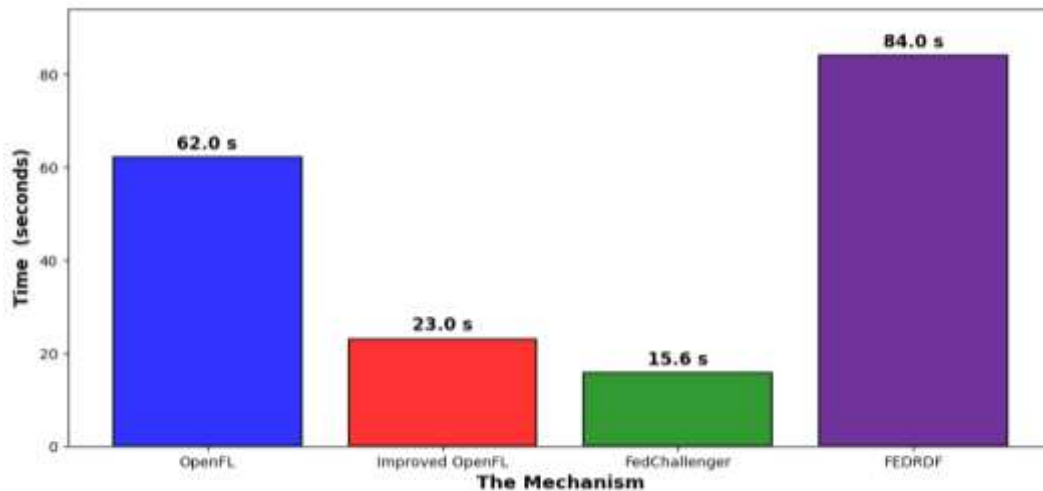
الشكل 3 كفاءة الآليات عند وجود (17%-20%-30%-40%) من العملاء كعملاء خبيثين

يوضح الشكل 3 كفاءة كل من OPENFL، OPENFL المحسنة، FEDCHALLENGER، FEDRDF وذلك عند وجود (40%-30%-20%-17%) من العملاء كعملاء خبيثين.

يوضح الرسم البياني الأول على اليسار كيف تدهورت الدقة بشكل كبير عند عدم وجود أي آلية لتجنب العقد الخبيثة ويعود سبب هذا التدهور الكبير إلى أن التعلم الموحد في عملية التجميع يعتمد على المتوسط الحسابي لحساب الوزن النهائي والذي سيتأثر بشكل واضح بالقيم الشاذة. توضح الرسوم البيانية أن الآليات الأربعة تمكنت من الحفاظ على كفاءة اختيار المشاركين الجيدين عند جميع نسب الهجوم المدروسة. حيث نلاحظ أن النموذج المجمع الناتج عن كل آلية من هذه الآليات استمر بالتحسن خلال جولات التعلم الموحد الثمانية رغم زيادة عدد المشاركين الخبيثين. تمكنت OPENFL الأصلية من تجنب المشاركين الخبيثين بشكل صحيح لأن جميع المشاركون يمتلكون بيانات متشابهة إحصائياً (كل مشارك يمتلك عينات لجميع صور الأرقام أو ما يعرف بالتوزيع المتجانس) مما جعل تقييم النماذج والتصويت عليها دقيقاً. أما الآلية المقترحة و FEDCHALLENGER فقد اعتمدتا على قياس توافق اتجاه أوزان النماذج باستخدام تشابه جيب التمام حيث بقيت أوزان المشاركين الجيدين متقاربة في الاتجاه في حين اختلفت اتجاهات الأوزان الناتجة عن هجوم Random Noise عن اتجاه الأوزان الجيدة الأمر الذي مكن الآليتين من التمييز بين التحديثات السليمة والشاذة عند جميع نسب الهجوم. استطاعت FEDRDF تجنب المشاركين الخبيثين عند جميع نسب الهجوم لأن الأوزان الصادرة عن العملاء الشرعيين تتجمع معاً بشكل طبيعي، مما يؤدي إلى ظهور كثافة عالية (تردد عالٍ) عند تحويلها إلى مجال التردد [10]. في المقابل، تضطر الأوزان الخبيثة التي تسعى لإحداث ضرر في النموذج إلى الابتعاد عن هذا التجمع الطبيعي، مما يجعلها تظهر متناثرة وبكثافة منخفضة في المجال الترددي [10]. تشير هذه النتائج إلى أن استبدال آلية التقييم المعتمدة على بيانات التحقق في OPENFL بقياس توافق اتجاه الأوزان لم يؤثر على قدرة الآلية في اختيار المشاركين. يمكن أن نلاحظ من الأشكال البيانية وجود فروقات بسيطة في المراحل الأولى من التدريب بين الآليات المختلفة ويعزى ذلك إلى التهيئة العشوائية الأولية لأوزان الشبكة العصبية في كل آلية ولكنها تتقارب تدريجياً مع التقدم بجولات التعلم، ما يهمنا أكثر هو استمرار التحسن بين جولة وأخرى لأنه يعني أن المشاركين الخبيثين لم يستطيعوا التأثير على النموذج الناتج وهو ما نجحت فيه جميع الآليات عند جميع نسب الهجوم.

السيناريو الثاني: تقييم أداء آليات تجنب هجمات التسميم من حيث الزمن

- نهدف في هذا السيناريو إلى توضيح أن عملية تحسين OPENFL ساهمت في تخفيض زمنها.
- يوضح الشكل 4 متوسط زمن تنفيذ كل آلية من الآليات السابقة خلال جولة واحدة بوجود 6 مشاركين



الشكل 4 متوسط زمن التنفيذ لكل آلية خلال جولة واحدة

تُظهر النتائج تفوقاً واضحاً لآلية OPENFL المحسنة على OPENFL الأصلية من حيث الكفاءة الزمنية، حيث بلغ متوسط زمن تنفيذ OPENFL (62) ثانية، في حين انخفض إلى (23) ثانية عند استخدام تشابه جيب التمام ويعود هذا التحسن إلى اختلاف منهجية تقييم أوزان النماذج بين الآليتين حيث تعتمد OPENFL الأصلية على اختبار الأوزان باستخدام بيانات تحقق (Validation Data)، وهي عملية تتطلب وقتاً حسابياً خاصة أن كل مشارك يقوم بتقييم نماذج جميع المشاركين الآخرين. في المقابل، تستبدل OPENFL المحسنة هذه العملية بحساب تشابه جيب التمام بين متجهات الأوزان، وهو إجراء رياضي مباشر يتميز بانخفاض تعقيده الحسابي وعدم حاجته إلى بيانات إضافية وقد أكدت نتائج المقارنة مع آلية FEDCHALLENGER هذه الملاحظة إذ حققت زمناً قدره (15.6) ثانية باعتمادها على تشابه جيب التمام، وهو ما يعزز أن استخدام تشابه جيب التمام يمثل خياراً فعالاً لتقليل الزمن مقارنة بالطريقة المعتمدة على تقييم النماذج باستخدام بيانات التحقق. يعود الفرق بالزمن بين OPENFL المحسنة و FEDCHALLENGER إلى أنه في OPENFL المحسنة كل مشارك سيقوم جميع المشاركين الآخرين أي يتم تنفيذ تشابه جيب التمام بعدد مرات أكثر مما هو عليه في FEDCHALLENGER. أما FEDRDF فقد سجلت أعلى زمن تنفيذ (84 ثانية) نتيجة الكلفة الحسابية الإضافية لتحويل الأوزان لكل طبقة من طبقات النموذج من مجالها الحقيقي إلى المجال الترددي باستخدام FFT أثناء عملية التجميع، مما يجعلها الأبطأ بين الآليات رغم كفاءتها في مقاومة الهجمات. تؤكد هذه النتائج أن التحسين المقترح نجح في تقليل الزمن مع المحافظة على الكفاءة وهو أحد الأهداف الرئيسية التي سعينا إليها.

السيناريو الثالث: تقييم أداء OPENFL الأصلية والمحسنة من حيث Gas Costs

نهدف في هذا السيناريو إلى توضيح أن عملية تحسين OPENFL لم تتسبب بزيادة التكلفة. يوضح الجدول 3 تكلفة تنفيذ الجولة الواحدة عند استخدام كل من OPENFL الأصلية والمحسنة أو بمعنى آخر كمية الغاز اللازمة لتنفيذ جولة التعلم بوجود الآلية مع تحويل هذه الكمية إلى ETH لتوضيح التكلفة المالية المقابلة.

الجدول (3) تكلفة تنفيذ الجولة الواحدة لكل من OPENFL الأصلية والمحسنة

الآلية	تكلفة الجولة
OPENFL ON ROPSTEN [4]	1,035,117gas=0.02070 ETH
OPENFL	1,029,591gas=0.02059 ETH
IMPROVED OPENFL	1,029,939gas=0.02060 ETH

في الدراسة [4] تم تنفيذ OPENFL على شبكة Ethereum اختبارية وهي ROPSTEN باستخدام محاكي ganache عبر وضع fork وبالتالي يمكننا مقارنة نتائجنا التي أجريناها محلياً على ganache مع نتائج هذه الدراسة لنستطيع الحكم على مدى قابلية تنفيذ OPENFL المحسنة عملياً وذلك لأننا لا نستطيع تنفيذها على شبكات Ethereum حقيقية كونها مدفوعة. نلاحظ أن تكلفة تنفيذ OPENFL على شبكة Ethereum اختبارية هو تقريباً 0.02 ETH وقد وضع الباحثون أن هذه التكلفة مناسبة لتنفيذ الآلية عملياً. عندما قمنا بتنفيذ الآليتين محلياً على ganache وجدنا أنها أيضاً تتطلب ما يقارب 0.02ETH مما يعني إمكانية تنفيذ هذه الآليات عملياً على شبكة Ethereum. ما يهمنا أكثر هو أن عملية التحسين لآلية OPENFL لم تتسبب بزيادة في تكلفة التنفيذ.

التحديات:

من أبرز التحديات التي واجهتنا هي قيود محاكي ganache الذي يقدم لنا 10 حسابات Ethereum مما يشكل عائقاً أمام اختبار فعالية OPENFL المحسنة عند زيادة عدد العقد، إضافة إلى عدم قدرتنا على تجريب OPENFL المحسنة على شبكات Ethereum حقيقية كونها مدفوعة.

5. الاستنتاجات والتوصيات:

توصلت هذه الدراسة إلى أن الآلية المُحسَّنة المقترحة، والتي تعتمد على مقياس تشابه جيب التمام (Cosine Similarity) ضمن إطار عمل OPENFL، تمثل نهجاً فعالاً لمعالجة مشكلة هجمات Random Noise Attack في أنظمة التعلم الموحد القائمة على سلاسل الكتل. فقد أظهرت النتائج أن استبدال آلية التحقق التقليدية المعتمدة على بيانات التحقق بمقياس تشابه رياضي مباشر أسهم في تبسيط عملية التقييم دون الإخلال بجودة النتائج. بينت التجارب أن الآلية المقترحة حافظت على الكفاءة، مما يدل على أن الاعتماد على اتجاه الأوزان (بدل اختبارها) يُعد مؤشراً كافياً للحكم على جودة التحديثات في هذا السياق.

كما أظهرت النتائج تحسناً ملحوظاً في التكلفة الزمنية بلغ (62.9%) مقارنة بالآلية الأصلية، وهو تحسن جوهري يعزز من ملائمة الآلية للتطبيق في البيئات التي تتطلب استجابة سريعة ويجعلها قادرة على منافسة آليات متقدمة مثل FEDCHALLENGER. في المقابل، لم يُسجل أي ارتفاع يُذكر في تكاليف التنفيذ (Gas Costs) على شبكة Ethereum، مما يؤكد أن التحسين المقترح لا يفرض عبئاً اقتصادياً إضافياً.

استناداً إلى ما توصلت إليه الدراسة من نتائج، يمكن تقديم التوصيات التالية:

1. اعتماد مقياس تشابه جيب التمام كطريقة تحقق في آليات حماية التعلم الموحد التي تستخدم طريقة التصويت على سلسلة الكتل خاصة في البيئات الحساسة للزمن، لما يوفره من تقليل كبير في زمن المعالجة دون التأثير على الدقة.

2. دمج الآلية المقترحة مع أنظمة السمعة والحوافز (المكافأة والعقوبة) لتعزيز موثوقية المشاركين والحد من تأثير العقد الخبيثة، بما يضمن استقرار النظام على المدى الطويل.
 3. توسيع نطاق التجارب لتشمل بيانات أكبر وأكثر تعقيداً من حيث عدد المشاركين وتنوع سلوكهم، بهدف تقييم قابلية التوسع والتحقق من استقرار الأداء في السيناريوهات الواقعية.
 4. دراسة أداء الآلية المقترحة في حالات الهجمات التعاونية للمشاركين الخبيثين، لتحديد حدود فعاليتها وتطوير آليات داعمة تزيد من متانتها في مثل هذه الظروف.
 5. إجراء تجارب إضافية باستخدام مجموعات بيانات ونماذج أكثر تعقيداً وأنواع أخرى من الهجمات، وتوزيع غير متجانس للبيانات لضمان إمكانية تعميم النتائج على تطبيقات عملية متنوعة.
 6. تنفيذ الآلية المقترحة على شبكات سلاسل كتل حقيقية، للحصول على تقييم أدق للتكلفة والأداء في ظروف تشغيل واقعية.
- وعليه، فإن العمل المستقبلي يمكن أن يركز على تطوير نماذج هجينة تجمع بين مقاييس تشابه متعددة وتقنيات كشف متقدمة، بما يعزز من قدرة الأنظمة على مقاومة الهجمات المعقدة وتحقيق أداء مستقر في البيئات اللامركزية واسعة النطاق.

References:

- [1] L. Shi, "A survey on federated learning: evolution, applications and challenges," in Proceedings of the 5th International Conference on Computing and Data Science, pp. 106–111, 2023.
- [2] J. Liu, J. Wu, "A comprehensive survey on blockchain technology and its applications," Highlights in Science, Engineering and Technology (CSIC), vol. 85, pp. 128–138, 2024.
- [3] G. Xia, J. Chen, C. Yu, J. MA "Poisoning attacks in federated learning: A survey," IEEE Access, vol. 11, pp. 10708–10722, 2023.
- [4] A. Wahrstätter, S. Khan, D. Svetinovic, "OPENFL : A scalable and secure decentralized federated learning system on the Ethereum blockchain," Internet of Things, vol. 26, 2024.
- [5] J. Zhu, J. Cao, D. Saxena, S. Jiang, H. Ferradi, "Blockchain-empowered federated learning: Challenges, solutions, and future directions," ACM Computing Surveys, vol. 55, no. 11, 2023.
- [6] Y. Chang, C. Fang, W. Sun, "A blockchain-based federated learning method for smart healthcare," Computational Intelligence and Neuroscience, vol. 2021 , 2021.
- [7] Z. Qin, X. Yan, M. Zhou, and S. Deng, "BlockDFL: A Blockchain-based Fully Decentralized Peer-to-Peer Federated Learning Framework," in Proceedings of the ACM Web Conference 2024 (WWW '24), Singapore, May 13–17, pp. 2914–2925, 2024.

- [8] X. Cao, M. Fang, J. Liu, and N. Z. Gong, "FLTrust: Byzantine-Robust Federated Learning via Trust Bootstrapping," Network and Distributed System Security Symposium (NDSS), 2021.
- [9] C. Fung, C. J. M. Yoon, and I. Beschastnikh, "The Limitations of Federated Learning in Sybil Settings," in Proceedings of the 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020), pp. 301–316, 2020
- [10] E. Mármol Campos, A. Gonzalez-Vidal, J. L. Hernández-Ramos, and A. Skarmeta, "FEDRDF : A Robust and Dynamic Aggregation Function Against Poisoning Attacks in Federated Learning," IEEE Transactions on Emerging Topics in Computing, vol. 13, no. 1, pp. 48–67, 2025.
- [11] M. A. Moyeen, K. Kaur, A. Agarwal, S. R. Manzano, M. Zaman, and N. Goel, "FedChallenger: A Robust Challenge-Response and Aggregation Strategy to Defend Poisoning Attacks in Federated Learning," IEEE Access, vol. 13, pp. 153866-153885, 2025.
- [12] A. Levy, B. R. Shalom, and M. Chalamish, "A guide to similarity measures and their data science applications," Journal of Big Data, vol. 12, 2025.