Ministry of Higher Education and
Scientific Research
University of Mosul
College of Computer Science and
Mathematics
Department of Computer Science

Lightweight Cyber Attack Intelligent Detection Model Based on Blockchain in IoT

**A Thesis Submitted to the Council of the College of
Computer Science and Mathematics
University of Mosul
as a Partial Fulfillment of Requirements
for the Degree of Doctor of Philosophy in
Computer Science**

By

Mahmood Subhy Mahmood Saeed

Supervised by

Dr. Najla Badie Ibraheem

2023 A.D. **1444 A.H.**

Abstract

Cyberspace is a complex environment consisting of heterogeneous technologies (i.e., Cloud Computing, Fog Computing, Internet of Things and so forth) resulting from interacting services, software and people on the Internet. It allows users to interact, share information, swap ideas, engage in social or discussion forums, play games, and conduct business, among many other activities. The biggest challenges facing cyberspace today are Cyber-attacks, which affect security and privacy services. However, many traditional security mechanisms provide protection and security services to solve these issues. Therefore, many researchers have been focused on solving security and privacy issues by integrating emerging technologies like (Artificial Intelligence, Blockchain, Cloud Computing, and Deep Learning).

Consequently, this thesis depended on the similar ideas above by proposing a Lightweight Intrusion Detection Model (LIDS-IoT) based on Deep Learning and Blockchain technologies provide a highly secure, authenticated, detection, and scalability in an IoT environment. The development of the proposed model passed through three stages.

The first stage includes developing Lightweight Intrusion Detection (LID) model based on a Sequential Multi-Layer Perceptron (MLP) Model. LID has the following characteristics lightweight, high accuracy, high speed in detection, and deals with a few features in Message Queuing Telemetry Transport (MQTT) protocol. The MQTTset dataset is utilized in training, validating, and testing the model. The achieved performance ratios of the proposed LID are measured by a number of features, accuracy and F1-score. The results of the experiments are as follows: for the balanced MQTTset dataset, the number of obtained features was 15 with accuracy (95.06) and F1-score (95.31). The number of obtained features for the unbalanced MQTTset dataset was 12 with accuracy (96.97) and F1-score (96.80). The obtained results have shown the efficiency of deep learning in improving the accuracy of an intrusion detection model by approximately 3.5% compared to other methods in the literature. In addition, the proposed methods reduced the number of features by around 50% of the total number of features, producing a LID model that can operate in a constrained environment. Moreover, the Rule-based strategy has been used to construct the signatures for attack classification to reduce the False Positive rate.

The second stage comprises deploying the developed LID model over the private network based on blockchain technology, which aims to eliminate

the issues of centralized detection methods, achieve scalability and authority. This process is achieved by implementing and designing a Lightweight, Practical Byzantine Fault Tolerance (LPBFT) consensus algorithm that improves the conventional (PBFT) algorithm. The obtained advantages of implementing the proposed LPBFT are a simpler message structure, does not need a primary server, low computation time, and consists of just two stages (request and reply). That makes it workable efficiently in IoT networks. Two scenarios have been applied to evaluate the performance of the LPBFT algorithm. In each scenario, one of the blockchain nodes is selected as a trainer, and the rest consider clients.

In the final stage, a LIDS-IoT (LID with the Classification Rules) is applied in a real physical environment (Raspberry Pi 4B). Four scenarios (Normal traffic with no attack, Malformed data attack, Bruteforce attack, and Slowite DoS attack) have been done to evaluate it. The experimental results have shown that the proposed LIDS-IoT has the ability to detect and classify three of five MQTT Broker attacks.

As a result, the proposed LIDS-IoT is one of the techniques producing acceptable performance in providing privacy and security services for the IoT environment.

وزارة التعليم العالي والبحث العلمي
جامعة الموصل
كلية علوم الحاسوب والرياضيات
قسم علوم الحاسوب

نموذج ذكي خفيف الوزن لكشف الهجوم السيبراني باعتماد Blockchain في انترنيت الاشياء

اطروحة مقدمة
الى مجلس كلية علوم الحاسوب والرياضيات في جامعة الموصل
كجزء من متطلبات نيل شهادة دكتوراه فلسفة في
علوم الحاسوب

من قبل

محمود صبحي محمود سعيد

بإشراف
ا.م.د. نجلاء بديع ابراهيم

١٤٤٤ هـ ٢٠٢٣ م

المستخلص

الفضاء السيبراني عبارة عن بيئة معقدة تتكون من تقنيات غير متجانسة (مثل الحوسبة السحابية والحوسبة الضبابية وإنترنت الأشياء وما إلى ذلك) الناتجة عن تفاعل الخدمات والبرامج والأشخاص على الإنترنت . يسمح للمستخدمين بالتفاعل ومشاركة المعلومات وتبادل الأفكار والمشاركة في المنتديات الاجتماعية أو منتديات المناقشة وممارسة الألعاب وممارسة الأعمال التجارية، من بين العديد من الأنشطة الأخرى .أكبر التحديات التي تواجه الفضاء السيبراني اليوم هي الهجمات الإلكترونية، والتي تؤثر على خدمات الأمان والخصوصية .ومع ذلك، توفر العديد من الآليات الأمنية التقليدية خدمات الحماية والأمن لحل هذه المشكلات .لذلك، ركز العديد من الباحثين على حل مشكلات الأمان والخصوصية من خلال دمج التقنيات الناشئة مثل (الذكاء الاصطناعي، وBlockchain، والحوسبة السحابية، والتعلم العميق) .

وبالتالي، اعتمدت هذه الأطروحة على الأفكار المماثلة المذكورة أعلاه من خلال اقتراح نموذج كشف التسلـــــل خفيف الـــــــوزن (LIDS-IoT) استنادًا إلى تقنيات التعلم العميق و Blockchainالتي توفر أمانًا عاليًا ومصادقًا واكتشافًا وقابلية للتوسع في بيئة إنترنت الأشياء .تم تطوير النموذج المقترح عبر ثلاث مراحل.

تتضمن المرحلة الأولى تطوير نموذج كشف التسلل خفيف الوزن (LID) بناءً على نموذج (MLP). يتميز LID بالخصائص التالية خفيف الوزن وعالي الدقة وسرعة عالية في الكشف ويتعامل مع بعض الميزات في بروتوكول (MQTT) . تُستخدم مجموعة بيانات MQTTsetفي التدريب والتحقق من صحة النموذج واختباره .يتم قياس نسب الأداء المحققة لـ LID المقترح بعدد الميزات المستخدمة والدقة وF1-score . كانت نتائج التجارب كما يلي: بالنسبة لمجموعة بيانات MQTTset المتوازنة ، كان عدد الميزات التي تم الحصول عليها ١٥ بدقة (٩٥,٠٦) وF1-score (95.31) . كان عدد الميزات التي تم الحصول عليها لمجموعة بيانات MQTTset غير المتوازنة ١٢ بدقة (٩٦,٩٧) و F1-score (96.80).أظهرت النتائج التي تم الحصول عليها كفاءة التعلم العميق في تحسين دقة نموذج كشف التسلل بحوالي ٣,٥٪ مقارنة بالطرق الأخرى في الأدبيات .بالإضافة إلى ذلك، خفضت الطرق المقترحة عدد الميزات بحوالي ٥٠٪ من إجمالي عدد الميزات، مما أدى إلى إنتاج نموذج LIDيمكن أن يعمل في بيئة مقيدة .علاوة على ذلك، تم استخدام الاستراتيجية المستندة إلى القواعد لإنشاء التواقيع لتصنيف الهجوم لتقليل معدل الإيجابي الكاذب.

تتضمن المرحلة الثانية نشر نموذج LID المطور على الشبكة الخاصة بناءً على تقنية blockchain ، والتي تهدف إلى القضاء على مشكلات طرق الكشف المركزية ، وتحقيق قابلية التوسع والسلطة. يتم تحقيق هذه العملية من خلال تنفيذ وتصميم خوارزمية إجماع خفيفة الوزن وعملية لتحمل الخطأ البيزنطي (LPBFT) التي تعمل على تحسين الخوارزمية التقليدية (PBFT) .المزايا التي تم الحصول عليها من تنفيذ LPBFT المقترح هي هيكل رسالة أبسط ، ولا يحتاج إلى خادم أساسي ، ووقت حساب منخفض ، وتتكون من مرحلتين فقط (الطلب والرد) .هذا يجعلها قابلة للتطبيق بكفاءة في شبكات إنترنت الأشياء .تم تطبيق سيناريو عدد اثنين لتقييم أداء خوارزمية LPBFT .في كل سيناريو ، يتم تحديد إحدى عقد blockchain كمدرب ، والباقي يعتبر العملاء.

في المرحلة النهائية، يتم تطبيق LIDS-IoT (LIDمع قواعد التصنيف) في بيئة مادية حقيقية . (Raspberry Pi 4B)تم إجراء أربعة سيناريوهات (حركة مرور عادية بدون هجوم ، وهجوم بيانات تالف ، وهجوم Bruteforce ، وهجوم Slowite DoS) لتقييمه. أظهرت النتائج التجريبية أن LIDS-IoT المقترح لديه القدرة على اكتشاف وتصنيف ثلاثة من خمسة هجمات MQTT . Brokerونتيجة لذلك ، فإن تقنية LIDS-IoT المقترحة هي إحدى التقنيات التي تنتج أداءً مقبولاً في توفير خدمات الخصوصية والأمن لبيئة إنترنت الأشياء.