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

Developing an IoT Lightweight Authentication System Based on IOTA Tangle Technology

**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

Sameera Abbas Fadhel Sheet

Supervised by

Assist. Prof. Dr. Ahmed Sami Nori Ahmed

2024 A.D. **1446 A.H.**

ABSTRACT

The most challenging threat that could face any Internet of Things environment is a cyber-attack, which may lead to severe damage to the services security of the whole IoT system. Nevertheless, many conventional security approaches are designed and implemented to provide protection and security services and address these challenges in the IoT environment. Each technology in the IoT environment has its limitations, most notably lightweight specifications as IoT components have limited computation power, the common weak point in IoT that causes security threats comes from unauthorized devices that perform various attacks on IoT systems.

Therefore, this thesis proposes a Lightweight Authentication Model for the Internet of Things (LAM-IoT) employing IOTA Tangle technology. This technology provides a highly secure authenticated facility and is more scalable and lightweight for the IoT environment.

The design of the proposed framework went through three main phases. The first phase includes selecting the most appropriate technology by comparing the most well-known technologies which include IOTA Tangle and blockchain. Two scenarios have been applied to evaluate the performance of the IOTA Tangle technology (using Private and Public Tangle) by measuring several metrics that reflect lightweight requirements which include CPU usage, energy consumption, bandwidth usage, and jitter. The results show a reduced need for PoW mining and the parallel processing capability of IOTA Tangle, which leads to lower CPU usage compared to blockchain technology and in terms of energy consumption.

Based on the findings of the first phase, a new, lightweight authentication scheme for smartphones has been presented in the second phase to validate the selection of IOTA Tangle. Moreover, digital assets including cryptographic keys, device data, and seeds are stored in a secure storage inside the IOTA Stronghold vault. IOTA Stronghold provides the Ed25519 data signatures algorithm for authentication

purposes. The obtained results showed promising features of the IOTA Tangle in the fulfillment of lightweight authentication requirements.

In the final phase, based on the findings of the first and second phases, a LAM-IoT is proposed utilizing IOTA Tangle and identity, which is a decentralized authentication technique. Employing a Decentralized Identifier (DID). The proposed LAM-IoT is evaluated using a practical implementation where Raspberry Pi with several connected sensors interrelates with a fog node connected to Tangle.

The proposed model is explored and validated through security and functionality and verified using the Syther tool. The finding shows the efficiency of the LAM-IoT and lightweight security management requirements are satisfied in the IoT environment and fulfill its requirements in terms of scalability, communication, and storage overhead compared with the existing studies, and can operate in a constrained environment. It is obvious that the LAM-IoT was performed better in terms of power consumption (213 mJoules) and it achieved the shortest authentication time (7.8 ms).

وزارة التعليم العالي والبحث العلمي
جامعة الموصل
كلية علوم الحاسوب والرياضيات

تطوير نظام مصادقة خفيف الوزن بالاعتماد على تقنية IOTA Tangle

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

من قبل
سميرة عباس فاضل شيت

بإشراف

أ. م. د. أحمد سامي نوري أحمد

٢٠٢٤ م ١٤٤٦هـ

المستخلص

إن التهديد الأكثر تحديًا الذي قد يواجه أي بيئة إنترنت الأشياء هو الهجوم الإلكتروني، والذي قد يؤدي إلى أضرار جسيمة لأمن الخدمات في نظام إنترنت الأشياء بأكمله. ومع ذلك، تم تصميم وتنفيذ العديد من مناهج الأمن التقليدية لتوفير خدمات الحماية والأمن ومعالجة هذه التحديات في بيئة إنترنت الأشياء. ولكل تقنية في بيئة إنترنت الأشياء محدداتها، وأبرز هذه المواصفات انها خفيفة الوزن حيث أن مكونات إنترنت الأشياءلديها قوة حسابية محدودة، ونقطة الضعف الشائعة في إنترنت الأشياء التي تسبب تهديدات أمنية تأتي من الأجهزة غير المصرح بها التي تنفذ هجمات مختلفة على أنظمة إنترنت الأشياء.

لذلك، تقترح هذه الأطروحة نموذج مصادقة خفيف الوزن لإنترنت الأشياء (LAM-IoT) باستخدام تقنية IOTA Tangle. توفر هذه التقنية تسهيلات مصادقة آمنة للغاية وأكثر قابلية للتطوير وخفيفة الوزن لبيئة إنترنت الأشياء.

مر تصميم الإطار المقترح بثلاث مراحل رئيسة، تتضمن المرحلة الأولى اختيار التكنولوجيا الأكثر ملاءمة من خلال مقارنة أكثر التقنيات شهرة والتي تشمل IOTA Tangle و Blockchain. تم تطبيق سيناريوهين لتقييم أداء تقنية IOTA Tangle (باستخدام Private and Public Tangle) من خلال قياس العديد من المقاييس التي تعكس متطلبات خفة الوزن والتي تشمل استخدام وحدة المعالجة المركزية واستهلاك الطاقة واستخدام النطاق الترددي والتذبذب. تظهر النتائج انخفاض الحاجة إلى تعدين PoW وقدرة المعالجة المتوازية لـ IOTA Tangle، مما يؤدي إلى انخفاض استخدام وحدة المعالجة المركزية مقارنة بتقنية blockchain ومن حيث استهلاك الطاقة.

بناءً على نتائج المرحلة الأولى، تم اقتراح مخطط مصادقة خفيف الوزن جديد للهواتف الذكية في المرحلة الثانية للتحقق من صحة اختيار IOTA Tangle. علاوة على ذلك، يتم تخزين الأصول الرقمية بما في ذلك المفاتيح التشفيرية وبيانات الجهاز والبذور في تخزين آمن داخل خزنة IOTA Stronghold. توفر IOTA Stronghold خوارزمية Ed25519 لتوقيع البيانات لأغراض المصادقة. أظهرت النتائج التي تم الحصول عليها ميزات واعدة لـ IOTA Tangle في تلبية متطلبات المصادقة خفيفة الوزن.

في المرحلة النهائية، بناءً على نتائج المرحلتين الأولى والثانية، تم اقتراح LAM-IoT باستخدام IOTA Tangle والهوية، وهي تقنية مصادقة لامركزية، باستخدام معرف لامركزي

(DID). تم تقييم LAM–IoT المقترح باستخدام تطبيق عملي حيث يرتبط Raspberry Pi مع العديد من أجهزة الاستشعار المتصلة بعقدة ضباب متصلة بـ Tangle.

تم استكشاف النموذج المقترح والتحقق من صحته من خلال الأمان والوظائف والتحقق منه باستخدام أداة Syther. تظهر النتائج كفاءة LAM– IoT بالإضافة الى تلبية متطلبات إدارة الأمان خفيفة الوزن في بيئة إنترنت الأشياء كما تلبي بمتطلباتها من حيث قابلية التوسع والاتصالات ونفقات التخزين مقارنة بالدراسات الحالية، ويمكن أن تعمل في بيئة مقيدة. من الواضح ان أداء LAM–IoT كان أفضل من حيث استهلاك الطاقة (٢١٣ مللي جول) كما حقق وقت اقصر للمصادقة (٧.٨ مللي ثانية).