نموذج لأمن انترنت الأشياء مبني على مبدأ الملكية واستخدام تقنية سلسة الكتل.

بيان هزاع هاشم البركاتي

بإشراف الدكتورة: هيا المقوشي

المستخلص

ظهرت إنترنت الأشياء كتقنية رائدة تضم عدداً هائلاً من الكيانات المرتبطة والتي شكلت ثورة للتحول الرقمي في مختلف المجالات. ومع ذلك فإن الطبيعة المعقدة لبيئة إنترنت الأشياء تقدم سطحاً غنياً للمهاجمين لاستغلال نقاط ضعفها وتهديد أصولها. وتعتبر بيانات الملكية لأجهزة انترنت الأشياء أحد الأصول الأساسية، والتي تدار عادة من قبل كيانات مركزية او أطراف وسيطة، والتي بدورها تتحكم بتخزين وتبادل البيانات بين الأطراف المشاركة. بالإضافة إلى أنها تعتبر إحدى العوامل لمعالجة متطلبات الأمان. إن الاعتماد على الكيانات المركزية بإدارة ملكية الأجهزة يشكل تهديداً أمنياً ومصدراً للهجمات الإلكترونية. لذا قد يكون تبني الطبيعة اللامركزية بتقنية سلسلة الكتل هو الحل الأمثل، حيث يمكن استغلال إمكانياتها لإدارة ملكية أجهزة إنترنت الأشياء بطريقة آمنة وموثوقة دون تدخل أي من الكيانات المركزية او الأطراف الوسيطة. ولذلك، تهدف هذه الأطروحة إلى اقتراح نموذج لإدارة ملكية أجهزة إنترنت الأشياء بطريقة آمنه مع تجاوز عيوب السلطة المركزية. النموذج المقترح (IoT of Trust) مبني على تقنية سلسلة الكتل باستخدام Ethereum smart contract. ويهدف النموذج لبناء ثقة متبادلة مع اتساق البيانات بين جميع الأطراف المشاركة، كذلك ضمان موثوقية وأصالة البيانات مع تخزينها بشكل دائم وغير قابل للتعديل. وقد أظهرت نتائج الاختبار أن نموذج (IoT of Trust) يفي بمتطلبات الأمان الأساسية وهي السرية والتكامل والتوافر. بالإضافة إلى تحقيق درجة عالية بشفافية البيانات واخفاء الهوية والتأكد من عدم انكار أي معامله تم تنفيذها وكذلك الحفاظ على سلامة البيانات وعدم التلاعب بها. إلى جانب ذلك عززت نتائج التقييم جدوى أداء النموذج في بيئة إنترنت الأشياء، حيث أن متوسط رسوم المعاملات أقل من دولار واحد أمريكي لكل منها ومتوسط وقت الاستجابة لاستدعاء البيانات المخزنة حوالي ٢٨ جزء من الثانية. كخطة مستقبلية نسعى لإجراء المزيد من الاختبارات للتحقق من جدوى النموذج، وذلك بتجربته على بيئة أكثر تحدي كبيئة Mainnet Ethereum network بالإضافة إلى اختباره على سيناريو منفذ على أرض الواقع.

An Ownership-based IoT Security Model Using Blockchain.

By
Bayan Hazzaa Hashem Al Barakati

Supervised by

Dr. Haya Almagwashi

Abstract

Internet of Things (IoT) has emerged as a leading technology involving an enormous number of entities. However, the complex nature of the IoT environment presents a rich surface for attackers to exploit its vulnerabilities and threaten its assets. The ownership of IoT devices is considered as one of the major assets, that is usually managed by centralized entities or Trusted Third Parties (TTP). IoT ownership is utilized to tackle some of the security requirements. Yet, relying on the centralized entity is a high risk as it can become the source of the attack itself. Hence, adopting the decentralized nature of blockchain technology might be the security game-changer, as it can potentially be utilized to manage the ownerships of IoT devices in a secure and decentralized manner without comprising central authorities or TTP.

The primary focus of this thesis is to provide end-to-end trust in ownership management in which the data is consistent among all participants. Therefore, we propose an Ownership-based IoT security model using blockchain, called IoT of Trust. The proposed model relies on the smart contract, which is deployed onto an Ethereum blockchain network. IoT of Trust intends to handle the central authority issue by utilizing the blockchain capabilities with respect to trusted authenticity, origin, and permanent storage. It plays the role of controlling the ownership functions securely throughout the device lifecycle, as well as acquiring trusted logs of the device from the current owner back to the origin.

The testing results demonstrate that IoT of Trust offers a significant degree of transparency, anonymity, immutability, and non-repudiation. In addition, the results of the evaluation reinforce the feasibility of the model's performance in the IoT environment, as the average of the transaction fee for the main transactions is less than 1 USD/each. In addition, the average response time for calling the stored data is minimal, which is about 0.28 seconds. The research was deployed on the Ethereum blockchain network; however, future work includes carrying out further testing to validate the proposed model on the Mainnet Ethereum network and operate it on a real-world smart IoT environment.