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

Design a Security System for IoT Applications based on Blockchain

**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

Shatha Abdulmunem Baker Ahmed

Supervised by

Assistant Professor

Dr. Ahmed Sami Nori

2022 A.D. **1443 A.H.**

Abstract

The Internet of Things (IoT) is a revolution that has transformed traditional living into a high-tech lifestyle. The IoT is a technology that allows a huge range of devices to be connected with each other and capture a big amount of data. Although the benefits of IoT are limitless, it faces a great challenge in providing security. Therefore, the criteria for IoT protection have become paramount. Security in IoT has drawn growing interest from both academic and industrial sectors to counter future risks and to provide effective and safe services.

Cryptographic algorithms are important defense mechanism that provides good security protection. In the recent years, various encryption lightweight algorithms have been presented to ensure the security of data transmitted via the IoT network. These algorithms are able to meet the requirements of IoT devices that have limited resources. A RECTANGLE lightweight block cipher algorithm has been proposed for system. Improvements were made to the algorithm by extending it using the 3D cipher architecture and modifying the algorithm for the key schedule. The improvement enhanced the algorithm's diffusion and confusion without growing block and key sizes. The experiments demonstrated that the proposed algorithm outperforms the original version, with a bit error rate of (51%) for both changes of plaintext and key.

To assess the randomness of proposed algorithm, randomness analysis was done by using the NIST statistical test suite include 15 tests and nine categories of data. 100 samples for each category of data was tested. NIST tests carried out under 1% significance level. The proposed algorithm's randomness analysis gave (27.48%) better results than the original algorithm.

In addition to security concerns, there are many other challenges to implementing IoT, for example centralization and scalability, which occur due to large numbers of networked objects. Therefore, there is an urgent need to provide a decentralized, secure and scalable environment to transform the path of IoT into it. One of the well-known example of the decentralized solutions is blockchain.

The blockchain is perhaps among the most significant technologies to emerge since the beginnings of the internet. It is the basic technology that behind Bitcoin and other crypto-currencies that have gotten a lot of attention in recent years. At its core, a blockchain is a distributed ledger which permits parties to conduct transactions with no need for a centralized authority. Blockchain is a sophisticated technology that decentralizes management and computing processes. It can address a many of IoT challenges, including security. It relies on a Proof of Work (PoW) concept, and a block is valid after the system has proof that miners have performed sufficient computing effort. Miners work separately and compete with one another to build the same block. As a consequence, all miners' efforts except the miner who find the solution becomes useless for each block, resulting in huge amounts of energy wasted.

The system proposes a consensus algorithm by distribute the PoW process among miners. Each node only finds a PoW for their little fraction of the searching area, resulting in no two miners putting in the same amount of effort to solve a single block. The consensus algorithm tested by using different scenarios, with different the level of difficulty and number of miners. Results evaluations demonstrate the algorithm has improved the time required to mine blocks to (77.442%, 91.716%) when the number of miners are 10, 20 respectively.

Furthermore, the system employs a decentralized Random Beacon (RB) to randomly select nodes to take part in the block notarization process that reducing the time required for block confirmation.

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

تصميم نظام امني لتطبيقات انترنت الاشياء باعتماد بلوكشين

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

من قبل

شذى عبدالمنعم بكر احمد

بإشراف

الاستاذ المساعد

د. احمد سامي نوري

1443 هـ

2022 م

الخلاصة

إنترنت الأشياء (IoT) هو ثورة حولت الحياة التقليدية إلى أسلوب حياة عالي التقنية. IoT هي تقنية تسمح لمجموعة كبيرة من الأجهزة بالاتصال ببعضها البعض والتقاط كمية كبيرة من البيانات. على الرغم من أن مزايا إنترنت الأشياء لا حدود لها، إلا أنها تواجه تحديًا كبيرًا في توفير الأمن، وبالتالي أصبحت معايير حماية إنترنت الأشياء ذات أهمية قصوى. جذب الأمن في إنترنت الأشياء اهتمامًا متزايدًا من كلا القطاعين الأكاديمي والصناعي لمواجهة المخاطر المستقبلية ولتوفير خدمات فعالة وآمنة.

تعد خوارزميات التشفير آلية دفاعية مهمة توفر حماية أمنية جيدة. في السنوات الأخيرة، تم تقديم خوارزميات تشفير خفيفة الوزن مختلفة لضمان أمان البيانات المنقولة عبر شبكة إنترنت الأشياء، وهذه الخوارزميات قادرة على تلبية متطلبات أجهزة إنترنت الأشياء ذات الموارد المحدودة. تم اقتراح خوارزمية تشفير كتلة خفيفة الوزن RECTANGLE للنظام. واجريت تحسينات على الخوارزمية من خلال توسيعها باستخدام بنية التشفير ثلاثية الأبعاد وتعديل خوارزمية جدولة المفتاح. عزز التحسين انتشار الخوارزمية والارتباك دون زيادة أحجام الكتلة والمفاتيح. أظهرت التجارب تفوق الخوارزمية المقترحة على الإصدار الأصلي ، حيث بلغ معدل الخطأ في البتات (51٪) لكل من التغييرات في النص العادي والمفتاح.

من اجل تقييم عشوائية الخوارزمية المقترحة، تم إجراء تحليل العشوائية باستخدام مجموعة الاختبار الإحصائي NIST التي تتضمن 15 اختبارًا وتسع فئات من البيانات. تم اختبار 100 عينة لكل فئة من البيانات. أجريت اختبارات NIST تحت مستوى أهمية 1٪. نتائج تحليل العشوائية للخوارزمية المقترحة اعطت نتائج أفضل بنسبة 27.48٪ من الخوارزمية الأصلية.

بالإضافة للمخاوف الأمنية هناك العديد من التحديات الأخرى التي تواجه تنفيذ إنترنت الأشياء، على سبيل المثال المركزية وقابلية التوسع والتي تحدث بسبب الأعداد الكبيرة من الاجهزة المتصلة بالشبكة. لذلك، ظهرت الحاجة الملحة لتوفير بيئة لامركزية وآمنة وقابلة

للتطوير لتحويل مسار إنترنت الأشياء إليه. أحد الأمثلة المعروفة للحلول اللامركزية هو blockchain.

ربما تكون blockchain من بين أهم التقنيات التي ظهرت منذ بدايات الإنترنت. إنها التكنولوجيا الأساسية التي كانت وراء Bitcoin والعملات المشفرة الأخرى التي حظيت باهتمام كبير في السنوات الأخيرة. في جوهرها ، blockchain عبارة عن سجل موزع يسمح للأطراف بإجراء معاملات دون الحاجة إلى سلطة مركزية. Blockchain هي تقنية متطورة تعمل على إضفاء اللامركزية على عمليات الإدارة والحوسبة، ويمكنها معالجة العديد من تحديات إنترنت الأشياء، بما في ذلك الأمان. يعتمد على إثبات مفهوم العمل، وتكون الكتلة صالحة بعد أن يثبت النظام أن المعدنين قد قاموا بجهد حوسبي كافٍ. يعمل عمال المناجم بشكل منفصل ويتنافسون مع بعضهم البعض لبناء نفس الكتلة. نتيجة لذلك، تصبح جهود جميع المعدنين باستثناء المعدن الذي يجد الحل عديمة الفائدة لكل كتلة ، مما يؤدي إلى إهدار كميات هائلة من الطاقة.

يقترح النظام خوارزمية إجماع من خلال توزيع عملية إثبات العمل بين المعدنين. تكتشف كل عقدة فقط PoW لجزءها الصغير من منطقة البحث، مما يؤدي إلى عدم بذل اثنين من المعدنين نفس القدر من الجهد لحل كتلة واحدة. تم اختبار خوارزمية الإجماع باستخدام سيناريوهات مختلفة، مع اختلاف مستوى الصعوبة وعدد المعدنين. توضح تقييمات النتائج أن الخوارزمية قد حسنت الوقت المطلوب لتعدين الكتل إلى (77.442٪ ، 91.716٪) عندما يكون عدد المعدنين 10، 20 على التوالي.

علاوة على ذلك، يستخدم النظام منارة عشوائية لامركزية (RB) لاختيار العقد بشكل عشوائي للمشاركة في عملية توثيق الكتلة التي تقلل الوقت المطلوب لتأكيد الكتلة.