University of Mosul
College of Engineering

Advanced Encryption Standard Improvement for Internet of Things

Alaa Salim Abdalrazzaq

Master Dissertation of Science in Computer Engineering / Computer Engineering

Supervised by

Assistant Professor Dr. Salah Abdulghani Jaro

2022 A.D. 1444 A.H.

Abstract

One of the most important communication technologies of our day is the Internet of Things (IoT). The IoT system faced issues with device power consumption, battery life, memory space, and cost of performance as a result of this advancement and expansion of IoT devices. Encryption algorithms are one of the most crucial ways to guarantee the confidentiality of data while it is being transmitted.

Advanced Encryption Standard (AES) is one of the most popular encryption algorithms. In this dissertation, the Tiny Advanced Encryption Standard (TAES) algorithm has been proposed with several possibilities to improve the AES algorithm's encryption speed and flexibility when used for small data. It is also proposed to achieve a high level of encryption and reduce the complexity of the algorithm.

Using the MATLAB program, the performance of the proposed algorithm was compared to that of the original AES algorithm on texts and images. The results showed that the proposed algorithm reduced the time required for encryption and decryption. It is interesting to note that the proposed algorithm was able to encrypt data from 4 bytes to a significant amount of bytes for text and images, throughput and speedup in encrypting and decrypting, signal-to-noise ratio (SNR), peak signal-to-noise ratio (pSNR), and mean square error (MSE) values were calculated. The results showed the proposed algorithm's advantage for each of these measurements.

From the results, it can be concluded that when the scenarios of the TAES algorithm were implemented on data with a size of 2048 bytes, 97.184%, 97.16 %, and 81.98%, respectively when

the first, second, third, and fourth scenarios of the proposed algorithm were applied. Additionally, throughput rates grew at a rate similar.

جامعة الموصل

كلية الهندسة

تحسين معيار التشفير المتقدم لإنترنيت الأشياء

الاء سالم عبد الرزاق

رسالة ماجستير علوم في هندسة الحاسوب / هندسة الحاسوب

بإشراف

الأستاذ المساعد الدكتور صلاح عبدالغني جارو

1444هـ 2022م

الملخص

من أهم تقنيات الاتصال في يومنا هذا هي تقنية إنترنت الأشياء (IoT) . و هو نظام يجمع بسلاسة بين العديد من الأجهزة والتقنيات غير المتجانسة دون تدخل بشري. تم إنشاء أنظمة المدن الذكية باستخدام إنترنت الأشياء لتحسين راحة الإنسان وزيادة انتاجيته .نتيجة لهذا التقدم والتوسع في أجهزة إنترنت الأشياء فقد واجه نظام إنترنت الأشياء (IoT) مشكلات تتعلق باستهلاك طاقة الجهاز وعمر البطارية القصير ومساحة الذاكرة المحددة وتكلفة المرتفعة للأداء و تزايد الهجمات الإلكترونية والمخاطر الأمنية. برز الأمن السيبراني كواحد من أهم جوانب إنترنت الأشياء. يهدف الأمن السيبراني إلى تقليل التهديدات على أنظمة الكمبيوتر من خلال حماية البيانات الحساسة وضمان الخصوصية أثناء الإرسال. نظرًا لدورها الحاسم في ضمان أمن الاتصالات ، تعد خوارزميات التشفير واحدة من أكثر الطرق أهمية لضمان سرية البيانات أثناء إرسالها.

يُطلق على أحد خوارزميات التشفير الأكثر استخدامًا معيار التشفير المتقدم (AES).تبدأ هذه الخوارزمية بـ 128 بت من البيانات ، ولكل خطوة تشفير 10 جولات ، مما يزيد من مدة التشفير. في هذه الرسالة ، تم اقتراح خوارزمية معيار التشفير المتقدم الصغير (TAES) مع العديد من الاحتمالات لتحسين سرعة تشفير خوارزمية AES و جعلها مرنة عند استخدامها للبيانات الصغيرة ، حيث يبدأ الإدخال عند 4 بايت ويصل إلى عدد غير محدود من البايتات .و يهدف هذا المقترح ايضا الى تحقيق مستوى عالٍ من التشفير وتقليل تعقيد الخوارزمية.

باستخدام برنامج MATLAB ، تمت مقارنة أداء الخوارزمية المقترحة بأداء خوارزمية AES الأصلية على النصوص والصور والأصوات. أظهرت النتائج أن الخوارزمية المقترحة قللت من الوقت اللازم للتشفير وفك التشفير. و ايضا يمكن ملاحظة أن الخوارزمية المقترحة كانت قادرة على تشفير البيانات من 4 بايت إلى كمية كبيرة من البايت لكل من النص والصور و أظهرت النتائج جودة الخوارزمية المقترحة لكل من الإنتاجية والتسريع في التشفير وفك التشفير ، ونسبة الإشارة إلى الضوضاء (SNR) ، وإشارة الذروة إلى الضوضاء (pSNR) ، ومتوسط قيم الخطأ التربيعي (MSE).

من النتائج يمكن الاستنتاج أنه عند تنفيذ السيناريو الأول للخوارزمية المقترحة على بيانات بحجم 2048 بايت ، زادت سرعة تنفيذ التشفير بنسبة 96.033٪. وفي السيناريو الثاني ارتفع بنسبة 97.185٪. وبلغت النسبة المئوية للسيناريو الثالث 97.16٪ ، فيما بلغت نسبة الزيادة النهائية للسيناريو الرابع 81.98٪. بالإضافة إلى ذلك ، نمت معدلات الإنتاجية بمعدل مماثل للقيم السابقة.