حماية بيانات إنترنت الأشياء باستخدام خوارزميات التشفير الهجين

مها رده الله الطلحي

أطروحة مقدمة لمتطلبات درجة ماجستير العلوم في علوم الحاسب الآلي

المشرف
د. خالد الصبحي

كلية الحاسبات وتقنية المعلومات جامعة الملك عبدالعزيز
جدة ، المملكة العربية السعودية جمادى الثانية ١٤٤٤ هـ - يناير ٢٠٢٣ م

خلاصة

إنترنت الأشياء (IoT) هي تقنية سريعة النمو أدت إلى تحديث حياة البشر وقدمت العديد من الفوائد في جميع أنحاء العالم. تقوم إنترنت الأشياء بتوصيل العديد من الكائنات عبر الإنترنت لنقل المعلومات وأداء المهام بناءً على معلومات المستشعر. أصبحت هذه التقنية مستخدمة على نطاق واسع في العديد من المجالات ، مثل المنازل الذكية والمدن الذكية والطب. مع هذه الثورة في تقنية إنترنت الأشياء وزيادة الطلب عليها ، أصبحت المخاوف الأمنية وسرية البيانات من الاهتمامات الهامة لمستهلكي تطبيقات إنترنت الأشياء. على وجه الخصوص ، إذا كانت تطبيقات إنترنت الأشياء تعتمد على إنتاج البيانات الضخمة ، فإن الحفاظ على أمانها يمثل تحديًا كبيرًا. تتمثل أهم طريقة لحماية البيانات من التهديدات الأمنية في تخزينها في شكل مشفر. في هذا البحث سوف ندرس ثلاث حالات. في الحالة (١) ، طبقنا خوارزمية تشفير هجينة مقترحة تتكون من نوعين من خوارزميات التشفير ، خوارزمية DES المتماثلة وخوارزمية RSA غير المتماثلة. يتم تطبيق هذا النهج على Mhealth ، وهي مجموعة بيانات كبيرة لإنترنت الأشياء ، لحمايتها من الوصول غير المصرح به أثناء تخزين البيانات. في الحالة (٢) ، يتم تطبيق تقنية ضغط البيانات قبل خوارزمية التشفير الهجين. هذا يقلل من مساحة التخزين المطلوبة وأوقات التشفير وفك التشفير. أخيرًا ، في الحالة (٣) ، نستخدم نموذج التعلم العميق ، نموذج التشفير التلقائي ، لاستخراج بعض ميزات البيانات الهامة والحساسة قبل تطبيق خوارزمية التشفير الهجين. تتم مقارنة الطرق الثلاثة عن طريق قياس وقت التشفير ووقت فك التشفير والإنتاجية. لقد قررنا أن الحالة (٣) هي الطريقة الأكثر فاعلية: فهي تحقق تشفيرًا وفك تشفيرًا أسرع بنسبة ١٠٪ من الحالة (2) ، والتي بدورها تكون أكثر كفاءة بنسبة ٤٩٪ من الحالة.(1)

الكلمة المفتاحية: خوارزمية التشفير الهجين ، البيانات الضخمة ، الضغط ، التشفير ، فك التشفير

IoT Data Protection Using Hybrid Cryptographic algorithms

by

Maha Ruddah allah Altalhi

A thesis submitted for the requirements of the degree of Master of Science in Computer Science

Advisor

Dr. Khalid Ateatallah Alsubhi

Faculty of Computing and Information Technology King Abdulaziz University
Jeddah, Saudi Arabia JumadaII1444 H-Jan2023 G

Abstract

The Internet of Things (IoT) is a fast-growing technology that has modernized human lives and provided numerous benefits worldwide. The IoT connects many objects over the Internet to transmit information and perform tasks based on sensor information. This technology has become widely used in many fields, such as smart homes, smart cities, and medicine. With this revolution in IoT technology and the increase in demand for it, security concerns and data confidentiality have become important concerns for consumers of IoT applications. In particular, if IoT applications depend on the production of big data, keeping it secure is a significant challenge. The most important way to protect data from security threats is to store it in encrypted form. In this research, we will study three cases. In Case (1), we apply a proposed hybrid cryptography algorithm consisting of two types of encryption algorithms, the symmetric DES algorithm, and the asymmetric RSA algorithm. This approach is applied to Mhealth, a big IoT dataset, to protect it from unauthorized access during data storage. In Case (2), a data compression technology is applied before the hybrid cryptography algorithm. This reduces both the required storage space and the encryption and decryption times. Finally, in Case (3), we use a deep learning model, the auto-encoder model, to extract some critical and sensitive data features before applying the hybrid cryptography algorithm. The three approaches are compared by measuring their encoding time, decoding time, and throughput. We determine that Case (3) is the most efficient approach: it achieves 10% faster encryption and decryption than Case (2), which is in turn 49% more efficient than Case (1).

Key Word:*Hybrid cryptography algorithm, big data, compression, encryption, decryption*