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

إجراء مضاد قائم على التشفير لأنترنت الأشياء

رسالة مقدمة
إلى مجلس كلية علوم الحاسوب والرياضيات في جامعة الموصل
كجزء من متطلبات نيل شهادة ماجستير علوم في
علوم الحاسوب

من قبل

امجد أنور محمدجميل محمود

بإشراف

أ.م.د. نجلاء بديع إبراهيم الدباغ

1444 هـ 2023 م

المُلَخَص

غطت تكنولوجيا أنترنت الأشياء (IoT) العديد من المجالات في الحياة ، إذ يتم تطبيق أنظمتها على نطاق واسع في بيئات مختلفة وتطبيقات مختلفة ، ومن تم ، تُعَدُّ أنظمة IoT تقنية مثيرة للاهتمام للعمل معها من خلال إشراك الأجهزة الذكية في كل مكان مثل الأجهزة المحمولة وأجهزة الاستشعار والمشغلات ..... إلخ . تسهم أنترنت الأشياء بصورة فعالة في تطبيقات المنازل الذكية والمباني الذكية والمدن الذكية وحركة المرور وأنظمة المراقبة والصحة و ... إلخ ، إن أجهزة أنترنت هي أجهزة مقيدة بالموارد من حيث (المعالج ، حجم الذاكرة ، الطاقة) ، وان بعض تطبيقات أنترنت الأشياء تتطلب التعامل مع كميات كبيرة من البيانات التي تجمعها أجهزة الاستشعار المرتبطة به ، قد تكون هذه البيانات حساسة .

مع تزايد الطلب لبيئة أنترنت الأشياء موثوقة وآمنة ، ولتعدد التهديدات الأمنية في اثناء نقل البيانات عبر الشبكات (الأنترنت) والنمو الهائل في عدد ونوع الهجمات التي يجب التعامل معها من قبل خبراء أمن البيانات من أجل حماية البيانات الحساسة ، ولوجود حالات خطر خارجي على السلامة العامة والأمن العام تستغل هجمات التشفير في المرافق العامة والخاصة لأسباب مختلفة ، أصبح تأمين بيانات تطبيقات أنترنت الأشياء الدافع الرئيسي للمصممين والمطورين والباحثين ؛ لذلك تركز هذه الرسالة على تأمين البيانات عن طريق تشفيرها .

اقترحت هذه الرسالة أقترح تصميم بيئة محاكاة لتطبيق مراقبة الازدحامات المرورية في المدينة الذكية، يختص التطبيق بمراقبة حركة المركبات داخل المسارات في المدن الذكية من خلال نشر حساسات في جميع المسارات ترتبط بأجهزة أنترنت الأشياء، تقوم بجمع البيانات من مسارات المدينة وإرسالها بصورة آمنة عن طريق تشفيرها، ويتصل التطبيق بالحوسبة المركزية الضبابية /الحافة عن طريق شبكة أنترنت الأشياء ، لتأمين بيانات التطبيق وتحقيق متطلبات الأمان لأنترنت الأشياء ، تم بناء خوارزمية تشفير انسيابي خفيفة الوزن كطريقة لحماية البيانات ، واعتُمِدْت مفاهيم الديناميكية والحمض النووي . إذ تم إدخال الديناميكية في جميع مراحل الخوارزمية ، واستخدم تقنية التشفير المرة الواحدة لتعيين مفتاح امن لعملية التشفير يتم توليد المفتاح باستخدام سجل إزاحة التغذية المرتدة الخطية الديناميكية ، ويتم حشر البيانات اللازمة لفك التشفير في النص المشفر لتنظيم عملية توزيع المفتاح لتقليل النطاق الترددي للشبكة .

تشير نتائج اختبار معدل خطا الرقم الثنائي لمجموعة من عينات النص الأصلي والمشفر الناتج انه قيمة مقاربة ل (0.5) ومجموعة من الاختبارات الإحصائية لمجموعة من عينات النص المشفر مقبولة والانتاجية ل (1 Kbyte = 110.706920 , 128 Kbyte = 111.672770 , 256 Kbyte = 112.162046) وإنَّ الخوارزمية المقترحة اجتازت جميع الاختبارات ولها أداء جيد وملائم لحماية البيانات في بيئة أنترنت الأشياء المقيدة .

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

Encryption-Based Countermeasure For Internet of Things

**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 Master of Science
in
Computer Science**

By

Amjad Anwer M. Jameel Al abbas
Supervised by

Assistant.Prof.Dr. Najla Badie Ibraheem

2023 A.D. **1444 A.H.**

Abstract

Internet of Things (IoT) technology has covered many fields in life, as its systems are widely applied in different environments and different applications, IoT systems are an interesting technology to work with by involving ubiquitous smart devices such as mobile devices and sensors And triggers.....etc. The Internet of Things contributes effectively to the applications of smart homes, smart buildings, smart cities, traffic, health and monitoring systems, etc. Large amounts of data collected by its associated sensors, this data may be sensitive.

With the increasing demand for a reliable and secure Internet of Things environment, the multiplicity of security threats during the transfer of data over networks (the Internet), the exponential growth in the number and type of attacks that must be dealt with by data security experts in order to protect sensitive data, and the existence of cases of external danger to public safety and security. public exploit cryptographic attacks in public and private facilities for various reasons, securing the data of IoT applications has become the main motivation for designers, developers and researchers; Therefore, this message focuses on securing data by encrypting it.

This thesis proposes designing a simulated environment for the application of monitoring traffic congestion in the smart city. The application is concerned with monitoring the movement of vehicles within lanes in smart cities by deploying sensors in all lanes linked to Internet of Things devices, which collect data from city lanes and send it securely by encrypting it. The application is connected to the Fog/Edge central computing through the Internet of Things network, to secure application data and meet the security requirements of the Internet of Things. The dynamic was entered in all stages of the algorithm, and used the one-time encryption technology to set a secure key for the encryption process. The key is generated using a dynamic linear feedback shift register, and the data necessary for decryption is crammed into the ciphertext to organize the key distribution process to reduce network bandwidth.

The results of testing the binary error rate for a group of samples of the original text and the resulting cipher indicate that it is a value close to (0.5), and a group of statistical tests for a group of samples of the ciphertext is acceptable and the throughput is (1 Kbyte = 110.706920 , 128 Kbyte = 111.672770 , 256 Kbyte = 112.162046) and that The proposed algorithm passes all tests and has good performance, which is suitable for data protection in a restricted IoT environment.