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


# An IoMT Security System based on DNA Cryptography

**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**

**Sadoon Hussein Abdullah Mohammed**

**Supervised by**

**Asst. Prof.Dr.Ahmed Sami Nori Ahmed**

**2024 A.D.** **1446 A.H**

# Abstract

The Internet of Thing 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 large, 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.Each technology in the IoT environment has its limitations, most notably lightweight specifications as IoT components have limited computation power, the common weak point in IoT that causes security threats comes from unauthorized devices that perform various attacks on IoT systems. From this perspective, the main idea behind this work is to use promising technologies like DNA (Deoxyribonucleic acid) Computing in order to provide a more robust security backbone for IoT platforms.One of the widespread environments of the IoT's is that which relates to patient data taken from sensors within the healthcare environment. Therefore, this the Internet of Medical Things (IoMT) environment was chosen for to work on within the thesis.

The proposed system design goes through four subsystems. The first subsystem represents the extraction of medical data from candidates (patients) called "nodes" which are monitored by biosensors. At first, the proposed lightweight authentication is done which in turn produces the private key for the encryption algorithm. Then the data is encrypted with the proposed lightweight algorithm based on DNA computation with the previously generated key. Then it is transferred via MQTT protocol to the second subsystem represented by the Raspberry Pi device which has an integrated broker or server and the data is processed and published to the authorized and subscribed end users (doctors) only (who are authorized according to a special algorithm) which is an application in Android which is the fourth subsystem after lightweight authentication between them and receives the data according to the common axes between them. Simultaneously, the data is sent and stored in the third subsystem which is the cloud dedicated to each patient according to a specific and lightweight authentication. All data collected from patients and doctors is securely stored on the Firebase cloud where the data is encrypted in DNA format to maintain data privacy and ensure the security of the healthcare system and medical privacy. When the patient needs to be warned, the end user (doctors) sends an encrypted message to the patient's screen which is

encrypted with a lightweight algorithm with a key generated based on the DNA properties represented by Short tandem repeat (STR) . In the same context, a lightweight algorithm was proposed to encrypt X-ray images patients, which is a lightweight algorithm based on the DNA properties.

The security system including the proposed algorithms, both authentication algorithms and encryption algorithms, were tested by several criteria. The experimental results showed that the authentication protocol proved to be completely secure, and this was proven using the Automated Validation of Internet Security Protocols (AVISPA) tool for authentication quality in all subsystems. In addition, the applied AVISPA tool showed that the proposed authentication protocol is attack proof against various types of attacks. The proposed algorithms (the proposed algorithm for patient data encryption in ESP, the STR key-based algorithm, and the proposed algorithm for X-ray encryption) met the requirements of lightweight security management in the IoT environment and met its requirements in terms of scalability, communication, and storage overhead compared to existing studies, and could operate in a constrained environment where the power consumption was (0.2µw,0.5µw,2.1µw) respectively, the memory consumption was (900Byte,2500 Byte,5900 Byte ) respectively, and the encryption cost was (0.28ms,0.12ms,2.13ms ) respectively. Also, a set of other criteria were passed, including Effect of the Key, Key Space Analysis, Key Sensitivity Analysis,Avalanch Effect,NIST Protocol Suite , the Throughput was (258kbps,258kbps,150kbps) respectively, and DNA properties of the criteria and other criteria.

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


# نظام مؤمن لأنترنيت الأشياء الطبية اعتماداً على تشفير الحمض النووي

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

من قبل
سعدون حسين عبدالله محمد

بإشراف
ا.م.د. أحمد سامي نوري أحمد

1446هـ 2024م

# المستخلص

يعد إنترنت الأشياء تقنية تسمح لمجموعة ضخمة من الأجهزة بالاتصال ببعضها البعض والتقاط كمية كبيرة من البيانات. وعلى الرغم من أن فوائد إنترنت الأشياء كبيرة، إلا أنه يواجه تحديًا كبيرًا في توفير الأمن. لذلك، أصبحت معايير حماية إنترنت الأشياء ذات أهمية قصوى. لقد جذب جانب الأمن في إنترنت الأشياء اهتمامًا متزايدًا من كل من القطاعين الأكاديمي والصناعي وذلك لمواجهة المخاطر المستقبلية وتوفير خدمات فعالة وآمنة. إذ ان كل تقنية في بيئة إنترنت الأشياء لها حدودها، وأبرزها المواصفات خفيفة الوزن حيث أن مكونات إنترنت الأشياء لها قوة حسابية محدودة. أما نقطة الضعف المشتركة في إنترنت الأشياء والتي تسبب تهديدات أمنية فتأتي من الأجهزة غير المصرح بها التي تنفذ هجمات مختلفة على أنظمته. من هذا المنظور، فإن الفكرة الرئيسية وراء هذا العمل هي استخدام تقنيات واعدة مثل حوسبة الحامض النووي (DNA) من أجل توفير العمود الفقري الأمني الأكثر قوة لمنصات إنترنت الأشياء. إحدى البيئات المنتشرة في إنترنت الأشياء هي تلك التي تتعلق ببيانات المرضى المأخوذة من أجهزة الاستشعار داخل بيئة الرعاية الصحية. بناءً على ذلك، أختيرت بيئة إنترنت الأشياء الطبية (IoMT) للعمل عليها في هذه الأطروحة.

يمر تصميم النظام المقترح باربع انظمة فرعية. النظام الفرعي الاول تمثل باستخراج البيانات الطبية المرشحين (المرضى) الذين يطلق عليهم "العقد" والتي تتم مراقبتها بأجهزة استشعار حيوية. في بداية الأمر، تتم المصادقة خفيفة الوزن المقترحة والتي بدورها تنتج المفتاح الخاص بخوارزمية التشفير. ثم يتم تشفير البيانات بخوارزمية خفيفة الوزن المقترحة والمستندة الى حساب الحامض النووي DNA مع المفتاح الناتج مسبقا. بعد ذلك يتم نقلها عبر برتوكول MQTT إلى النظام الفرعي الثاني المتمثل بجهاز Raspberry Pi الذي يحتوي على وسيط او خادم مدمج وتتم معالجة البيانات التي يتم نشرها الى المستخدمين النهائيين (الاطباء) المخولين والمشتركين فقط (والتي تم تخوليهم حسب خوارزمية خاصة) والتي تمثل تطبيق في الاندرويد وهو النظام الفرعي الرابع بعد مصادقة خفيفة الوزن بينهم ويستلم البيانات حسب المحاور المشترك بينهم بها. وبالتزامن ترسل وتخزن البيانات في النظام الفرعي الثالث والذي هو عبارة عن السحابة المخصصة لكل مريض حسب مصادقة خفيفة و محددة. تخزن جميع البيانات المجمعة من المرضى والأطباء بشكل آمن على سحابة Firebase حيث تكون البيانات مشفرة بصيغة الحامض النووي DNA للمحافظة على خصوصية البيانات وضمان أمان نظام الرعاية الصحية

والخصوصية الطبية. وعند الحاجة إلى تحذير المريض، يرسل المستخدم النهائي (الأطباء) رسالة مشفرة الى شاشة المريض والتي تشفر بخوارزمية خفيفة الوزن مع مفتاح يولّد اعتماداً على خصائص الحامض النووي DNA والممثلة بتكرار ترادف قصير STR وفي نفس السياق تم اقتراح خوارزمية خفيفة الوزن لتشفير صور الأشعة السينية (X-Ray) للمرضى ، وهي خوارزمية خفيفة الوزن ومستندة الى خصائص النووي DNA ايضا.

تم اختيار النظام الامني المتضمن للخوارزميات المقترحة سواء خوارزميات المصادقة او خوارزميات التشفير بعدة معايير. وأظهرت النتائج التجريبية أن بروتوكول المصادقة أثبت أنه آمن تمامًا، حيث تم إثبات ذلك باستخدام أداة AVISPA لجودة المصادقة في جميع الانظمة الفرعية. بالإضافة إلى ذلك، أظهرت أداة AVISPA المطبقة أن بروتوكول المصادقة المقترح هو منيع على الهجوم ضد أنواع مختلفة من الهجمات. اما الخوارزميات المقترحة (الخوارزمية المقترحة لتشفير بيانات المريض في ESP والخوارزمية المستند على مفتاح STR والخوارزمية المقترحة لتشفير الأشعة السينية)، فهي توافق متطلبات إدارة الأمان خفيفة الوزن في بيئة إنترنت الأشياء وتلبي متطلباتها من حيث قابلية التوسع والاتصال ونفقات التخزين مقارنة بالدراسات الحالية، ويمكن أن تعمل في بيئة مقيدة حيث بلغ استهلاك الطاقة (0.2µw,0.5µw,2.1µw) واستهلاك الذاكرة (900Byte,2500 Byte,5900 Byte) وزمن التشفير (0.28ms,0.12ms,2.13ms) جميعها على التوالي. كذلك تم اجتياز مجموعة من المعايير الاخرى منها تأثير المفتاح وتحليل فضاء المفتاح وتحليل حساسية المفتاح وتاثير الانهيار الجليدي واختبار وحزمة NIST وكانت الانتاجية (258kbps,258kbps,150kbps) على التوالي،علاوةً على معايير خاصة بخصائص الحامض النووي DNA ومعايير أخرى.