

# الهيكل الأمن لإنترنت الأشياء الطبية القائم على الحوسبة الضبابية

تهاني سعيد المحمادي

إشراف

د. سهير الشهري - د. سابين طاهر

## المستخلص

تقدم خدمة إنترنت الأشياء الطبية حلاً مبتكرة لحياة صحية، مما يؤدي إلى تغييرات جذرية في جوانب حياتنا. حيث يتم تمكين مزودي الرعاية الصحية من متابعة مرضاهم باستمرار وعن بعد في العديد من الحالات الطبية خارج المستشفيات ومكاتب مقدمي الرعاية الصحية. تساعد أنظمة وتطبيقات إنترنت الأشياء الطبية إلى زيادة توفر خدمات الرعاية الصحية الجيدة وسهولة الوصول إليها بتكلفة مناسبة. من ناحية أخرى، تولد أجهزة إنترنت الأشياء الطبية كمية كبيرة من البيانات المتنوعة في الوقت الفعلي، وهي حساسة للغاية. وبالتالي، فإن تأمين البيانات الطبية هو مطلب أساسي عند تطوير معماريات إنترنت الأشياء الطبية. ومع ذلك، فإن المعماريات التي يتم تطويرها في الأبحاث لديها العديد من المشكلات الأمنية.

للتصدي لتحدي أمن البيانات في إنترنت الأشياء الطبية، تمت دراسة دمج الحوسبة الضبابية وإنترنت الأشياء الطبية كحل جديد وناشئ. وبحماية البيانات، يعني ذلك أن البيانات الطبية يتم تخزينها في عقد الضباب ونقلها إلى السحابة بطريقة آمنة لمنع أي وصول غير مصرح به. في هذه البحث، نقترح تصميم معمارية آمنة تعتمد على سحابة الضباب لإنترنت الأشياء الطبية تدعم التشفير القائم على السمات لحماية البيانات الطبية. نتحقق من جدوى العمارة المقترحة ومقدرة النظام على مواجهة التهديدات الأمنية.

تظهر نتائج البحث جدوى اعتماد التطبيق القائم على الضباب في حماية البيانات الطبية مع الحفاظ على موارد أجهزة إنترنت الأشياء الطبية، والقدرة على منع الهجمات الأمنية المختلفة.

# **A Secure Fog-Cloud Based Architecture for MIoT**

**Tahani Saeed Almehmadi**

**Supervised By  
Dr. Suhair Alshehri and Dr. Sabeen Tahir**

## **ABSTRACT**

Medical Internet of Things (MIoT) offers innovative solutions to a healthier life, making radical changes in people's lives. Healthcare providers are enabled to continuously and remotely monitor their patients for many medical issues outside hospitals and healthcare providers' offices. MIoT systems and applications lead to increase availability, accessibility, quality, and cost-effectiveness of healthcare services. On the other hand, MIoT devices generate a large amount of diverse real-time data, which is highly sensitive. Thus, securing medical data is an essential requirement when developing MIoT architectures. However, the MIoT architectures being developed in the literature have many security issues.

To address the challenge of data security in MIoT, the integration of fog computing and MIoT is studied as an emerging and appropriate solution. By data security, it means that medical data is stored in fog nodes and transferred to the cloud in a secure manner to prevent any unauthorized access. In this research, we propose a secure fog-cloud based architecture for MIoT supporting ciphertext-policy attribute-based encryption (CP-ABE) to protect medical data. We investigate the feasibility of the proposed architecture and the ability of the system to encounter security threats.

Our research results demonstrate the feasibility of adopting the fog-based implementation in protecting medical data while conserving MIoT resources, and the capability to prevent various security attacks.