تتشرف كلية الدراسات العليا وكلية تقنية المعلومات بدعوتكم لحضور

مناقشة رسالة ماجستير

العنوان

بروتوكول مصادقة وتأسيس مفتاح تشفير لأنظمة الرعاية الصحية الذكية المقيدة بالاعتماد على دالة مادية غير قابلة للاستنساخ

للطالب

(عبد الله صالح الكوشلي)

المشرف
(د. فرج الصلابي)
كلية تقنية المعلومات

المكان والزمان

الساعة (1:30)
يوم الاثنين الموافق 18 أبريل 2022
E1 - 1021

الملخص

تعد أنظمة الرعاية الصحية الذكية أحد أهم تطبيقات إنترنت الأشياء. هذه الأنظمة تفيد العديد من فئات المجتمع وتوفر تحسينات ملحوظة لخدمات الرعاية الصحية. أنظمة الرعاية الصحية الذكية تكون عرضة للعديد من التهديدات والاختراقات الأمنية لأنها تعمل دون إشراف لفترات طويلة من الوقت، كما أن عملية التواصل فيها عبر قنوات عامة غير آمنة. بالإضافة إلى ذلك، في العديد من تطبيقات هذه الأنظمة، عقد الاستشعار تكون مزروعة داخل الجسم أو ذا حجم مصغر، ومقيدة الموارد. تحتم علينا المخاطر المحتملة من هذه التهديدات على حياة المرضى أو الأفراد أن نعطي تأمين الاتصالات في هذه الأنظمة أهمية قصوى. هذه الأطروحة توفر حلاً لمثل هذه الأنظمة يقوم بتأمين قنوات الاتصال فيها، من الطرف الى الطرف، وذلك باقتراح تصميم ابداعي لبروتوكول مصادقة وتأسيس مفتاح تشفير. الهدف الرئيسي للبروتوكول هو دراسة كيفية استخدام الدالة المادية الغير قابلة للاستنساخ كأساس للثقة ذو أعباء قليلة على النظام. لإنجاز الأهداف المرجوة، صمم البروتوكول حسب متطلبات أمنية صارمة، كما تمت الاستفادة من ضعف الدالة المادية غير القابلة للنسخ أمام هجوم النمذجة باستخدام التعلم الآلي بالإضافة إلى استخدام آلية السقاطة. كشفت عمليتا التحقق والتحليل للبروتوكول المقترح أنه مرشح مناسب لأنظمة الرعاية الصحية الذكية ذات الموارد المحدودة. تصميم البروتوكول المقترح له أيضًا تأثير على جوانب مهمة أخرى مثل إخفاء هوية عقد الاستشعار وسيناريو فقدان الجهاز الوسيط.

الكلمات المفتاحية: المصادقة وتأسيس مفتاح تشفير، السرية التامة الأمامية، الدالة المادية الغير قابلة للاستنساخ، أساس الثقة، أنظمة الرعاية الصحية الذكية، محدودة الموارد.