الجمهورية الجزئرية الدَيموقراطية الشَعبية
République Algérienne Démocratique et Populaire
وزارة التَعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة البليدة 1
Université de BLIDA 1
كليَة العلوم
Faculté des Sciences
قسم الإعلام الآلي
Département d'Informatique

Mémoire de Fin d'Études

En vue d'obtention du diplôme de Master

Option : Sécurité des Systèmes d'Information
&
Système Informatique et Réseau

Conception et développement d'un schéma d'authentification basé sur la technologie blockchain dans l'Internet des Objets

Réalisé par :

Mounir HABABOU
Hichem BENHAMMOU

Organisme d'accueil :

Présidente :	Mme.N. TOUBALINE	(USDB)
Examinateur :	Mr. Y. DOUGA	(USDB)
Promotrice :	Mme. S. AROUSSI	(USDB)
Encadreur :	Mr. H. KHEMISSA	(CERIST)

Remerciement

Tout d'abord, nous remercions ALLAH de nous avoir donné la patience et l'énergie pour réaliser ce travail.

Nos plus sincère remerciements pour notre Promotrice Madame Aroussi Sanaa pour la confiance que vous nous avez accordée, et les conseils et remarques que vous nous avez donner, Et de nous avoir orienté, corrigé notre travail et encouragé, nous avoir orienté. Nous avons acquis beaucoup de connaissance et savoir-faire bénéfique au cours de nos discussions

Nous tenant à remercie tout particulièrement Monsieur Khemissa hamza attaché de recherche à CERIST et promoteur de thèse, de nous avoir orienté.

Nous aimerions exprimer notre gratitude à tous les chercheurs et spécialistes, [les membres de jurée] qui ont pris le temps de discuter des différent problème et solution de notre sujet. Chacun de ces échanges nous a aidé à faire avancer notre projet.

Et nous remercions nos amis qui nous ont aidés avec des idées et des encouragements, nous citons notamment cher ami : Mehdi Nacer KERKAR.

Résumé

L'évolution de l'Internet des objets (Internet of Things, IoT) transforme les perceptions traditionnelles de l'Internet existant en un concept d'appareils intelligents qui interagissent les uns avec les autres. Les réseaux de capteurs sans fil jouent un rôle clé et prennent en charge divers domaines d'application IoT comme la e-santé. Les problèmes de sécurité sont, cependant,undes obstacles à leur utilisation, l'authentification des différentes entités interconnectées et la gestion des entités lors de l'authentification est une partie majeure de ce problème. Dans notre travail, nous proposons un schéma d'authentification compatible avec la faible puissance de calcul des appareils IoT connectés et ses ressources limitées. Notre schéma est basé sur la technologie blockchain qui offre un haut niveau de sécurité et assure la sécurité des identités du nœud participant dans le réseau. Les analyses de sécurité effectuées montrent que le schéma a une résistance contre plusieurs attaques telles que l'usurpation d'identité et l'attaque Dos.
Mots-clés : Internet des objets (IoT), E-santé, authentification, Blockchain.

Abstract

The evolution of the Internet of Things (IoT) transforms traditional perceptions of the existing Internet into a concept of smart devices that interact with each other. Wireless sensor networks play a key role and support various IoT application domains such as the e-health. Security concerns are, however, an obstacle to their use, the authentication of different interconnected entities among these problems, and the management of identities during authentication is a major part of this problem, in our work we propose a authentication scheme which is compatible with the low computing power of connected IoT devices and its limited resources, the scheme is based on Blockchain technology which offers a high level of security and ensures the security of the identities of the participating nodes in the network, Security analyzes we have done on our proposed scheme shows that the scheme has resistance against several attacks such as impersonation and Dos attack.

Keywords: Internet of things (IoT), E-health, authentication, Blockchain.

ملخّص

أدى تطور إنترنت الأشياء إلى تحويل التصورات التقليدية للإنترنت الحالي إلى مفهوم الأجهزة الذكية التي تتفاعل مع بعضها البعض. تلعب شبكات الاستشعار اللاسلكية دورًا رئيسيًا وتدعم مجالات تطبيقات إنترنت الأشياء المختلفة مثل العلاج الإلكتروني. ومع ذلك ، فإن المخاوف الأمنية هي عقبة أمام استخدامها ، ومصادقة الأجهزة المترابطة المختلفة من بين هذه المشاكل ، وإدارة الهويات أثناء المصادقة هي جزء رئيسي من هذه المشكلة ، في عملنا نقترح نظام مصادقة متوافق مع قوة الحوسبة المنخفضة للأجهزة المتصلة ومحدودية مواردها ، يعتمد المخطط على تقنية البلوكشين التي توفر مستوى عالٍ من الأمان وتضمن أمان هويات الأجهزة المشاركة في الشبكة ، والتحليلات الأمنية التي أجريناها على المخطط يُظهر أنَ المخطط المقترح لديه مقاومة ضد عدة هجمات مثل انتحال الهوية وهجوم الحرمان من الخدمة.

الكلمات المفتاحية: أنترنتالأشياء ،العلاجالإلكتروني،البلوكشين.

Table des matières