SOUTENANCE DE THÈSE

Monsieur Djamel Eddine KOUICEM

Soutiendra sa thèse de **doctorat** sur le sujet :

Sécurité de l'internet des objets
pour les systèmes de systèmes

Unité de recherche : HEUDIASYC UMR CNRS 7253

Le jeudi 21 novembre 2019 à 9h30
À l'UTC, centre Pierre Guillaumat, amphi L103

Devant le jury composé de :

M^me^ Dominique Gaiti, professeur des universités, université de technologie de Troyes

M. Pascal Urien, professeur des universités, télécom-Paristech

M. Hossam Afifi, professeur, Télécom-SudParis

M. Ken Chen, professeur des universités, université Paris 13

M. Hicham Lakhlef, maître de conférences, université de technologie de Compiègne, laboratoire Heudiasyc

M. Aziz Moukrim, professeur des universités, université de technologie de Compiègne, laboratoire Heudiasyc

M. Abdelmadjid Bouabdallah, professeur des universités, université de technologie de Compiègne, laboratoire Heudiasyc

Abstract

The Internet of things (IoT) is a new technology that aims to connect billions of physical devices to the Internet. These objects can be engaged in complex relationships including the composition and collaboration with other independent and heterogeneous systems in order to provide new functionalities, thus leading to the so-called systems-of-systems (SoS).
Currently, Security is one of the top challenges that hinder the future development of IoT. Indeed, IoT objects are deployed in open environments, which are subject to various kind of malicious attacks. In addition, the huge number of connected objects and the limitation of their resources make the security in IoT very difficult to achieve.
In this thesis, we focus on the application of lightweight cryptographic approaches and blockchain technology to address security problems in IoT, namely: authentication and trust management.
First, we were interested on some kind of IoT applications where we need to control remotely the execution of smart actuators using IoT devices. To solve this problem, we proposed an efficient and fine-grained access control solution, based on the Attribute Based Encryption (ABE) mechanism and one-way hash chains. Using formal security tools, we demonstrated the security of our scheme against malicious attacks.
Second, we tackled the problem of authentication in IoT based fog computing environments. Existing authentication techniques do not consider latency constraints introduced in the context of fog computing architecture. In addition, some of them do not provide mutual authentication between devices and fog servers. To overcome these challenges, we proposed a novel, efficient and lightweight mutual authentication scheme based on blockchain technology and secret sharing technique. We demonstrated the efficiency of our authentication scheme through extensive simulations.
The third problem treated in this work is the trust management in IoT. Existing trust management protocols do not meet the new requirements introduced in IoT such as heterogeneity, mobility and scalability. To address these challenges, we proposed a new scalable trust management protocol based on consortium blockchain technology and fog computing paradigm, with mobility support. Our solution allows IoT devices to accurately assess and share trust recommendations about other devices in a scalable way without referring to any pre-trusted entity. We confirmed the efficiency of our proposal through theoretical analysis and extensive simulations. Finally, we showed that our protocol outperforms existing solutions especially in terms of scalability, mobility support, communication and computation.

Résumé

l'internet des objets (IoT) est une nouvelle technologie qui vise à connecter des milliards d'objets physiques à Internet. Ces objets peuvent être engagés dans des relations complexes, notamment la composition et la collaboration avec d'autres systèmes indépendants et hétérogènes, afin de fournir de nouvelles fonctionnalités, conduisant ainsi à ce que l'on appelle les systèmes de systèmes (SoS).
Les composants de l'IoT communiquent et collaborent dans des environnements distribués et dynamiques, confrontés à plusieurs problèmes de sécurité de grande ampleur. La sécurité est considérée parmi les enjeux majeurs de l'IoT et soulève des défis liés aux contraintes de capacité de calcul et stockage ainsi que le très grand nombre des objets connectés.
Dans cette thèse, nous nous intéressons à l'application des outils cryptographiques ainsi que la technologie blockchain pour résoudre les problèmes de sécurité dans l'IoT, à savoir: l'authentification et la gestion de confiance. Dans un premier lieu, nous nous sommes intéressés au problème du contrôle d'accès distant des actionneurs intelligents utilisant des dispositifs IoT. Pour addresser ce problème, nous avons proposé une solution de contrôle d'accès efficace et à granularité fine, basée sur le mécanisme ABE (Attribute Based Encryption) et des chaînes de hachage. À l'aide d'outils formels d'analyse de sécurité, nous avons démontré la sécurité de notre protocole face aux attaques malveillantes. Dans un deuxième lieu, nous avons adressé le problème d'authentification dans les applications IoT basé sur le paradigme du fog computing. Nous avons proposé un nouveau protocole d'authentification mutuelle efficace qui est basé sur la technologie blockchain et la cryptographie à seuil. Dans notre solution, les objets IoT et les serveurs de fog n'ont besoin que de quelques informations à stocker pour vérifier l'authenticité de chaque objet du

système. L’authentification est effectuée seulement sur la bordure du réseau sans passer par des entités externes. Ainsi, la latence et la capacité de stockage sont réduites au minimum. Enfin, dans notre troisième contribution, nous avons proposé un nouveau protocole de gestion de réputation basé sur la technologie blockchain et le fog computing, avec la prise en charge de la mobilité des objets connectés. Notre protocole permet aux objets IoT d'évaluer et de partager avec précision la réputation relative aux autres objets de manière scalable, sans se recourir à une entité de confiance. Nous avons confirmé l'efficacité de notre protocole par des analyses théoriques et des simulations approfondies. Nous avons montré que notre protocole surpasse les solutions existantes, notamment en matière de scalabilité, prise en charge de la mobilité, la communication et le calcul.