UNIVERSITE SIDI MOHAMED BEN ABDELLAH
FACULTE DES SCIENCES DHAR EL MAHRAZ
FES

AVIS DE SOUTENANCE DE THESE

Le Doyen de la Faculté des Sciences Dhar El Mahraz –Fès – annonce que

Mr**: ISHIMWE NGABO Christophe**

Soutiendra **: le 04/05/2019** à **10 H** Lieu **: Salle de Réunion de Biologie**

Une thèse intitulée :

Secure Integration of the Wireless Sensor Networks with the Cloud Infrastructure. Case Study: Smart Cities

En vue d'obtenir le Doctorat

FD : Sciences et Technologies de l'Information et de la Communication (STIC)
Spécialité : Informatique

	NOM ET PRENOM	GRADE	ETABLISSEMENT
Président	Pr. BELLAFKIH Mostafa	PES	Institut National des Postes et des Télécommunications - Rabat
Directeurs de thèse	Pr. EL BEQQALI Omar	PES	Faculté des Sciences Dhar El Mahraz - Fès
Rapporteurs	Pr. HEDABOU Mustapha	PH	ENSA- Université Cadi Ayyad - Safi
	Pr. HAYAR Aawatif	PES	ENSEM – Université Hassan II - Casablanca
	Pr. CHENFOUR Noureddine	PES	Faculté des Sciences Dhar El Mahraz - Fès
Membres	Pr. EL KOUCH Rachid	PES	Institut National des Postes et des Télécommunications- Rabat
	Pr. Ahmed LBATH	Professeur des Universités	Université Grenoble Alpes- France

Résumé :

Cette thèse considère l'intégration des réseaux de capteurs sans fil avec le cloud computing. Dans un réseau de capteurs sans fil, les protocoles réseaux nécessaires pour envoyer des données d'un nœud à un autre ne sont pas identiques aux protocoles qui assurent le routage sur l'internet. Face à cette hétérogénéité de deux réseaux, nous avons proposé une solution architecturale divisant l'ensemble du système en différents couches physiques et logiques. Logiquement, le réseau de capteur sans fil est accédé à travers une passerelle (connectée physiquement à la station de base du réseau de capteur sans fil) depuis le réseau externe, donc cette passerelle est un point intermédiaire entre le réseau de capteur sans fil et le cloud ainsi que les utilisateurs finaux. Pour que le réseau de capteur sans fil, le cloud ainsi que les utilisateurs finaux puissent communiquer, nous avons recouru à l'utilisation d'une technologie interopérable (middleware) dont son choix a été l'objet d'une étude comparative entre les technologies d'interopérabilité les plus connues. Java RMI a été identifié comme meilleur middleware pour l'architecture proposé contre CORBA et les web services.
Pour la sécurité de l'intégration, nous avons proposé une solution visant la confidentialité de l'intégration, basée sur l'utilisation des algorithmes de chiffrement homomorphe. En posant des hypothèses, nous avons pu sélectionner le chiffrement de Domingo-Ferrer qui exige que le message initial à chiffrer sous forme d'un nombre entier doit être scindé systématiquement en plusieurs fragment de nombre. Donc le nombre de fragment est l'un des paramètres déterminant le niveau de sécurité de cet algorithme. Pour l'implémentation effectuée dans cette thèse, nous avons considéré 4 cas. Pour chaque cas, 10 000 données collectées par un nœud capteur ont été envoyé vers le cloud, dans le but d'évaluer l'impact de la fragmentation du message initial sur l'état de la batterie du nœud capteur. Premièrement, les données étaient en texte clair, après 10 000 paquets, le niveau de la batterie avait chuté de 1%. Deuxièmement, les messages étaient chiffrés avec deux fragments au départ et le niveau de la batterie a baissé de 6% après que 10 000 paquets aient été envoyé. Pour le troisième et le quatrième cas, les messages étaient aussi chiffrés avec respectivement trois et quatre fragments avant leur chiffrement, les niveaux de la batterie ont chuté de 7% et 8% respectivement pour ces deux derniers cas.
D'après la RADEEF (Régie Autonomie intercommunale de Distribution de l'Eau et d'Electricité de Fès), elle a les moyens pour savoir si un câble électrique est cassé et à quel endroit exact se trouvant la coupure mais par contre elle n'a pas des moyens pour savoir si un poteau lumineux ou électrique est dangereusement incliné voire même tombé. Afin d'implémenter l'architecture proposée précédemment dans cette thèse, nous avons pensé à une application de smart city qui consister à la surveillance des poteaux lumineux ou de transmission électrique. En fixant un nœud capteur embarquant l'accéléromètre triaxial sur un tour, nous avons pu déterminer l'angle d'inclinaison entre le tour et le sol. Les valeurs x, y et z données par l'accélération triaxial nous ont permis d'établir une relation mathématique pour calculer cet angle d'inclinaison. Pour valider cette application, nous avons comparé les angles calculés par cette application et les angles mesurés, nous avons constaté que l'incertitude est de l'ordre de 1°.

Mots clés :

Réseaux de capteurs sans fil, Cloud Computing, Villes Intelligentes, Chiffrement Homomorphe, Systèmes distribués.

SECURE INTEGRATION OF THE WIRELESS SENSOR NETWORKS WITH THE CLOUD INFRASTRUCTURE. CASE STUDY: SMART CITIES

Abstract:

This doctoral dissertation proposes the integration of wireless sensor networks with cloud computing. The wireless sensor network and the cloud (located on the external network such as the internet or intranet) are heterogeneous. Accordingly, the network protocols used to route data from one sensor node to another in a wireless sensor network differ from the routing protocols found on the internet. As result, we proposed an architectural solution dividing the whole system into different physical and logical layers. Logically, the wireless sensor network is reached through a gateway (physically connected to the wireless sensor network base station) from the external network, so this gateway mediates between the wireless sensor network, cloud as well as end users. To ensure communication in this system, we proposed the using of interoperable technology (middleware). Therefore, a comparative study has been conducted in order to pick out the middleware required for this integration. Among tree middleware best known (CORBA, Java RMI and Web Services), Java RMI has been identified as the best middleware for the proposed architecture.

About the security of integration, we proposed a solution related to data privacy of the whole system, based on the use of homomorphic encryption algorithms. After some assumptions, we picked out Domingo-Ferrer's cryptosystem, which requires the initial message to be encrypted as an integer must be systematically split into several fragment of numbers. Therefore, it should be noted that the number of fragments is related to the desired level of security. For the implementation carried out in this thesis, we considered 4 cases. For each case, 10,000 data collected by a sensor node were sent to the cloud, in order to evaluate the impact of fragmentation of the initial message on the battery state of the sensor node. First, the data was in plain text, after 10,000 packets, the battery level had dropped by 1%. Secondly, the messages were encrypted with two fragments initially and the battery level dropped by 6% after 10,000 packets were sent. For the third and fourth cases, the messages were also encrypted with respectively three and four fragments before their encryption, battery levels dropped by 7% and 8% respectively for the last two cases studies.

According to RADEEF (Régie Autonomie intercommunale de Distribution de l'Eau et d'Electricité de Fès), they have some ways to recognize the breakage of an electrical cable and exactly the location of the breakage but they have no way to recognize whether an electrical or light pole is dangerously inclined or even fallen. In order to implement the proposed architecture previously in this thesis, we thought about designing a smart city application sensing the tilt angle over poles. The implementation requires attaching a sensor node embedding the triaxial accelerometer on a pole, so that the end user can determine the angle of inclination between the pole and the ground. The x, y and z values given by the triaxial acceleration allowed us to establish a mathematical relation to calculate this angle of inclination. To validate this prototype, we compared the sensed angles and the measured angles, as result we found that the average error is about of 1°.

Key Words:
Wireless Sensor Networks, Cloud Computing, Smart Cities, Homomorphic Encryption, Distributed System.