CLERMONT AUVERGNE INP Isima

Rapport d'élève Ingénieur
Projet de troisième année

Filière : **Sécurité** et **réseaux**

SMARTHOUSE

Présenté par : **KHEDHAOURIA Eliès & MARCELET Paul**

Responsable Isima : Monsieur **Alexandre GUITTON**

Date de soutenance : **02/07/2024**

Campus des Cézeaux . 1 rue de la Chébarde . TSA 60125 . 63178 Aubière CEDEX

Remerciements

Table des matières

Table des figures

Résumé

Dans le cadre de notre **projet de fin d'études**, nous avons conçu et développé un **système de maison intelligente** capable de transmettre **des données en temps réel de manière sécurisée** vers un serveur distant. L'objectif principal est de mettre en place un **système de monitoring avancé**, permettant à un propriétaire de superviser et d'analyser les données générées par ses équipements connectés.

Pour garantir **l'intégrité et la confidentialité des échanges**, nous avons implémenté une **communication sécurisée basée sur des certificats SSL/TLS** et le protocole **MQTTs**, assurant ainsi une transmission chiffrée et authentifiée entre la maison et le serveur.

Les données collectées par les capteurs sont stockées dans une **base de données à série temporelle** (InfluxDB), spécialement optimisée pour le traitement et l'analyse de données en flux continu.

Une **API centralisée**, développée en **Laravel**, a été mise en place afin de :

— **Gérer la création des propriétaires** et l'association sécurisée de leurs équipements.

— **Automatiser la génération et la signature des certificats** pour garantir une authentification fiable.

— **Offrir une interface d'accès aux données**, permettant aux utilisateurs de récupérer **des données en temps réel ou historiques**, selon différents filtres appliqués à la base de données.

Enfin, une **interface graphique interactive**, développée en **Qt**, permet aux utilisateurs de **visualiser les données en temps réel** sous forme de **graphiques dynamiques**. Cette interface interagit directement avec l'API afin de récupérer et d'afficher **les données filtrées**, qu'elles soient en temps réel ou issues d'une période spécifique dans le passé.

Ce projet intègre **des technologies modernes et des concepts avancés en sécurité, IoT, gestion des bases de données et visualisation de données en temps réel**, assurant ainsi une **infrastructure robuste, fiable et évolutive**.

Abstract

As part of our **final-year engineering project**, we designed and developed a **smart home system** capable of securely transmitting **real-time data** to a remote server. The main objective is to implement an **advanced monitoring system** that allows a homeowner to monitor and analyze data generated by their connected devices.

To ensure **data integrity and confidentiality**, we implemented a **secure communication protocol based on SSL/TLS certificates** and the **MQTTs protocol**, providing encrypted and authenticated communication between the home and the server.

Sensor data is stored in a **time-series database** (InfluxDB), optimized for real-time data processing and analysis.

A **centralized API**, developed in **Laravel**, has been implemented to:

— **Manage the creation of homeowners** and the secure association of their devices.

— **Automate the generation and signing of certificates** to ensure reliable authentication.

— **Provide a data access interface**, allowing users to retrieve **real-time or historical data** based on various filters applied to the database.

Finally, an **interactive graphical interface**, developed in **Qt**, allows users to **visualize real-time data** using **dynamic graphs**. This interface directly interacts with the API to retrieve and display **filtered data**, whether in real-time or from a specific historical period.

This project integrates **modern technologies and advanced concepts in security, IoT, database management, and real-time data visualization**, ensuring a **robust, reliable, and scalable infrastructure**.

Chapter 1

Introduction

La **domotique** représente aujourd'hui un enjeu majeur dans le domaine des innovations technologiques. Avec l'essor des **maisons connectées** et des **IOTs**, les utilisateurs peuvent désormais **surveiller** et **contrôler** leur domicile à distance, leur assurant ainsi une amélioration significative en termes de **sécurité**, **d'efficacité énérgétique** et de **confort**. Cette évolution s'inscrit dans un contexte plus large dans lequel l'automatisation et la connectivité jouent un rôle crucial dans notre quotidien.
Le **monitoring à distance** des équipements d'une maison constitue un axe fondamental de la domotique moderne. Il permet aux propriétaires d'obtenir une **vue globale de l'état de leur habitation en temps réel**. Cela joue un rôle crucial dans plusieurs domaines:

- Il permet de **sécuriser** un domicile, permettant par exemple la détéction d'intrusion ainsi que la prévention des cambriolages
- Il permet également une **optimisation énérgétique** du domicile, par le biais de l'automatisation des objets connectés, en fonction d'horraires programmés, afin d'optimiser la consommation d'énergie.
- Il permet enfin **un confort et un contrôle à distance**, offrant aux propriétaires la possibilité d'activer ou de désactiver certains dispositifs sans être physiquement présent.

Si ces avancées technologiques offrent des opportunités considérables, elles soulèvent néanmoins une problématique critique: **la sécurisation des dispositifs IoTs et du transfert des données**. Aujourd'hui, de nombreux objets connectés sont déployés avec des failles de sécurité importantes souvent négligées par les fabricants et les utilisateurs. Des outils comme **Shodan**, un moteur de recherche spécialisé dans l'identification des appareils connectés exposés sur Internet, mettent en évidence la vulnérabilité de nombreux systèmes IoTs accessibles sans protection adéquate. Cette situation constitue un risque majeur, rendant possible des cyberattaques capables de compromettre **l'intégrité** et **la confidentialité** des données échangées.
Ce rapport décrit une architecture, solution à cette problématique en explorant l'une des applications majeures de la domotique: **le monitoring à distance des capteurs d'une maison connectée, ainsi que l'établissement d'une communication sécurisée et authentifiée entre celle-ci et un serveur distant**. L'objectif est de permettre aux utilisateurs de récupérer des **données en temps réel**, issues de capteurs de leur domicile tout en garantissant **une transmission chiffrée** afin de protéger les échanges contre d'éventuelles interceptions malveillantes. C'est à partir de cela que l'on peut définir une problématique à laquelle la solution doit répondre: **Comment développer un système de monitoring en temps réel pour une maison connectée, garantissant la sécurité de la transmission des données tout en renforcant l'authentification des équipements IoTs ?**

Chapter 2

Contexte du Projet

2.1 Analyse du besoin et définition des objectifs

Lorsqu'un résident quitte son domicile, il peut être préoccupé par l'état de sa maison, se demandant si une lumière a été éteinte ou si une fenêtre a été correctement fermée. Ces préoccupations sont légitimes, d'autant plus les statistiques récentes indiquent une augmentation des cambriolages de logements en France. En effet au 30 juin 2024, les forces de sécurité ont enregistré une hausse de 4% des cambriolages de logements sur les douze derniers mois [1]. Cette tendance souligne la nécessité de renforcer les dispositifs de sécurité pour protéger les habitations.
Parallèlement, la proliférations des dispositifs IOT dans les foyers pose des défis non négligeables en matière de cybersécurité. Bien que ces technologies offrent des avantages indéniables en termes de confort et d'efficacité énergetiques, elles peuvent constituées des points d'entrée pour les cybercriminelles si elle ne sont pas correctement sécurisées. Il est ainsi essentiel de garantir que seuls les propriétaires autorisés aient accès à ces dispositifs et que les données transmises soient protégés contre toute altération ou interception malveillante.
Fâce à ces constats, notre projet vise à développer une solution permettant la transimission sécurisée issues de capteurs IoT d'une maison vers un serveur distant. Cette solution devra assurer l'authentification des dispositifs, garantir l'intégrité ainsi que la confidentialité des données, et ainsi permettre aux propriétaires de surveiller à distance l'état de leur domicile en temps réel.

2.2 Organisation de la conception à la création

Dans le cadre du développement de ce projet, nous avons adopté une approche structurée en plusieurs phases allant de la simulation initiale de l'environnement domotique jusqu'à la mise en place d'une infrastructure de communication sécurisée et fiable.

Phase 1: Simulation de l'environnement domotique et émission des données
Avant de mettre en place l'architecture réseau et serveur, nous avons débuté par la simulation logicielle de la maison connectée, en programmant un environnement permettant la génération de données de divers capteurs (température, humidité, lumière...). Cette simulation développée en **Python**,modélise une maison contenant divers équipements Iots et capteurs emettant des séries de données à temps réel.
L'objectif principal de cette étape était de tester l'envoie de séries de données, à intervalle régulier, au sein d'un serveur distant (Phase suivante), en utilisant le protocole de communication **MQTT**. A ce

1. source: `https://www.interieur.gouv.fr/actualites/actualites-du-ministere/analyse-conjoncturelle-des-crimes-et-delits` et `https://mobile.interieur.gouv.fr/Interstats/Actualites/Info-Rapide-n-43-La-delinquance-enregistree-par-la-police-et-l`

moment là, la transmission s'effectuait sans authentification ni chiffrement, nous permettant ainsi, de valider l'intégralité du transport, la récéption au serveur et d'évaluer aussi les performances du protocole.

Phase 2: Mise en place de l'infrastructure serveur
Une fois la simulation fonctionnelle, nous avons déployé une **infrastructure serveur** sous une machine virtuelle **Ubuntu**, utilisant l'hyperviseur **Virtualbox** avec un accès par pont en configuration réseau. Ce serveur assure le rôle de récépteur des données envoyées par la maison connectée.
Afin de permettre la récéption ainsi que le sotckage des données, nous avons mit en place plusieurs composants essentiels:

- **Mosquitto**: Un broker **MQTT** permettant la gestion des messages entres les maisons connectées et le serveur aux divers topics.
- **InfluxDB**: Une **base de données à séries temporelles**, choisie pour sa capacité à stocker et traiter efficacement des flux de données en temps réel.
- **Telegraf**: Un agent de collecte des données utilisé pour formaliser et structure les données recues depuis le **Broker** avant leur insertion dans la base de données.

À la fin de cette étape, après configuration des composantes, l'infrastructure était fonctionnelle, mais vulnérable : les données envoyées par les capteurs n'étaient pas protégées et n'importe quel utilisateur pouvait intercepter ou publier des messages MQTT sur le serveur, compromettant ainsi l'intégrité du système.

Phase 3: Sécurisation des échanges et authentifications des Maisons
Afin de garantir l'**authenticité des émetteurs** et de protéger les données échangées, nous avons implémenté une **authentification basée sur des certificats SSL/TLS** pour le protocole MQTT. Cette sécurisation repose sur **l'utilisation de certificats clients** généré par une autorité de certifcation interne au serveur, l'exigence d'une **authentification mutuelle** entre la maison et le serveur pour toute communication MQTT ainsi que le **chiffrement des échanges** grâce à TLS emêchant toute interception des données transmises.
Ce mécanisme permet ainsi de **garantir l'identité des dispositifs connectés** et d'empêcher ainsi toute inteception des données par un acteur non autorisé.

Phase 4 : Développement d'une API centralisant l'accès aux données
Afin de faciliter l'accès aux données, d'éviter une exposition directe du broker MQTT et aussi de permettre par la suite la création d'interfaces fonctionnant sur divers plateformes, nous avons concu une **API Rest sous laravel**, jouant deux rôles importants:

- **API de relais:**

Chapter 3

État de l'Art

3.1 Technologies existantes

3.2 Solutions alternatives et justification des choix

Chapter 4

Conception et Implémentation

4.1 Infrastructure et Environnement de Développement

4.1.1 Simulation du serveur et architecture réseau

Déploiement d'un Broker MQTT sécurisé

Intégration d'une base de données à séries temporelles

Formalisation des données entre Mosquitto et InfluxDB

4.1.2 Modélisation et Simulation d'une Maison Connectée

Conception de l'architecture logicielle de la simulation

Implémentation du protocole MQTTs

Structuration et formalisation des données échangées

4.2 Mise en place d'une API Web

4.2.1 Architecture logicielle de l'API et choix technologiques

4.2.2 Automatisation de l'authentification des maisons

Mise en place d'une base de données MySQL

Signature automatique des certificats

4.2.3 Filtrage et récupération des données

Communication avec InfluxDB API

4.3 Surveillance des données avec une interface graphique

4.3.1 Architecture logicielle de l'application SmartHouse Monitoring

4.3.2 Intégration et communication avec l'API Web

Authentification des maisons

Affichage des données récupérées

Chapter 5

Résultats et Discussion

5.1 Situation à la fin de l'étude

5.2 Analyse des résultats obtenus

Chapter 6

Conclusion

6.1 Conclusion du projet

6.2 Limites et améliorations possibles

Appendix A

Annexes

A.1 Lexique

A.2 Bibliographie

A.3 Webographie

Bibliography