Ecole Doctorale C2MP

« Chimie Mécanique. Matériaux Physique » - n° 606

Laboratoire Matériaux, Optique, Photonique et Système LMOPS,
Université de Lorraine, Metz, France.

DOCTOR of UNIVERSITE de LORRAINE
Major : Physics

Presented by

Carine ZARAKET

DISTRIBUTED RENEWABLE ENERGY RESOURCES ENABLEMENT BASED ON A SECURE AND VERSATILE ELECTRICITY TRADING ARCHITECTURE

December 1, 2022

Jury Members :

Président de jury	**Bruno ALLARD**	**Pr, AMPERE, Université de Lyon, Lyon, France**
Rapporteurs	**Cécile BELLEUDY**	**Ass. Pr, LEAT, Université de Nice, Nice, France**
	Fabienne NOUVEL/HUZEL	**Ass. Pr, IETR, INSA Rennes, Rennes, France**
Directeurs de thèse	**Michel AILLERIE**	**Pr, LMOPS, Université de Lorraine, Metz, France**
	Panagiotis PAPAGIORGAS	**Pr, University of West Attica, Athens, Greece**
Examinateurs	**Alexandre DE BERNARDINIS**	**Pr, LMOPS, Université de Lorraine, Metz, France**

Ecole Doctorale C2MP

« Chimie Mécanique. Matériaux Physique » - n° 606

Laboratoire Matériaux, Optique, Photonique et Système LMOPS,
Université de Lorraine, Metz, France.

Thèse pour l'obtention du titre de

DOCTEUR de l'UNIVERSITE de LORRAINE
Mention : Physique

Présentée Par

Carine ZARAKET

DÉVELOPPEMENT D'UNE ARCHITECTURE SÉCURISÉE ET POLYVALENTE D'ÉCHANGE D'ÉLECTRICITÉ D'ORIGINE RENOUVELABLE DANS UNE APPROCHE SMART-GRID

1 Decembre, 2022

Membres du Jury :

Président de jury	**Bruno ALLARD**	**Pr, AMPERE, Université de Lyon, Lyon, France**
Rapporteurs	**Cécile BELLEUDY**	**MCF-HDR, LEAT, Université de Nice, Nice, France**
	Fabienne NOUVEL/HUZEL	**MCF-HDR, IETR, INSA Rennes, Rennes, France**
Directeurs de thèse	**Michel AILLERIE**	**Pr, LMOPS, Université de Lorraine, Metz, France**
	Panagiotis PAPAGIORGAS	**Pr, University of West Attica, Athens, Greece**
Examinateurs	**Alexandre DE BERNARDINIS**	**Pr, LMOPS, Université de Lorraine, Metz, France**

Acknowledgments

This research work was done in collaboration between Laboratoire Matériaux Optiques Photoniques et Systèmes, LMOPS, de l'Université de Lorraine & West Attica University.

At the end of this work, I would like to express my sincere thanks to all the people who contributed to its realization and made it possible, through their support and advice, to bring it to a successful conclusion.

First of all, I would like to thank my supervisor, Prof. Michel Aillerie, who throughout my journey of 4 years at Lorraine University, has provided me with everything I could have ever asked for. His research rationale with clear focus was truly a guiding light during my Ph.D. I am very grateful to him for the thought-provoking discussions, sharing his broad knowledge and experience in every aspect of Renewables.

It is a privilege for me to have worked with Prof. Papageorgas Panagiotis, supervisor of this thesis, not only for his enlightening advice and generous support, but also thanks to his kindness and kindness. I thank him for welcoming me into the great "West Attica University" family, for his huge experience in IoT and blockchain and the precious time he devoted to me for scientific discussions throughout this work.

I would also like to thank Prof. Cécile Belleudy from Université de Nice, France and Prof. Fabienne Nouvel from INSA Rennes, France for agreeing to be the rapporteur for my thesis. Thank you for the time you have spent on this manuscript and also for the comments, the constructive remarks that you have made to improve it.

I am very happy that Pr. Bruno Allard from Université de Lyon, France and Prof. Alexandre De Bernardinis from Université de Lorraine, France have accepted to examine my thesis work. I hope to have the opportunity to work with you in the future.

A big thanks to all my friends Nikolaos Peladarinos, Efthymios Tserepas and Dr. Kyriakos Agavanakis. It has been a great privilege to be able to work with them on different research projects, share our ideas and perspectives during my thesis work and have countless fun moment that I will always cherish. A very special thanks to my close friends for supporting and encouraging

me during the hard time. You all have a special place in my heart and I hope our friendship lasts forever.

Most importantly, I would like to thank my beloved parents from the bottom of my heart for their unconditional love, support and guidance throughout my life. A special thanks to my sister and brother for their support encouragement and motivation. This thesis would not have been possible without your support all along the way. Last but not least, I would like to thank God for giving me the strength, courage, enthusiasm, knowledge, ability and opportunity to undertake this research study and to persevere and finish it successfully.

Abstract

Information and communication technologies (ICTs), adopted by the Smart Grid (SG), have been used to improve the control of the power system beyond that implemented in the conventional grid. Todays the objectives are, among others, to enable efficient integration of the renewable energy resources (RES), to maintain security of energy supply and to encourage the future energy market. As a result, the implementation of such a system requires the exchange of data between legacy and new smart grid applications. To make this possible, a versatile communication platform is required, so the main question that is answered in this thesis is: what would such a platform be?

The objective of this work is to design, implement and evaluate a low-cost, open-source, resilient telemetry gateway platform capable of integrating existing and future smart grid applications. This platform is optimized and tested using a variety of simulation, analysis, real implementation and prototypes tools.

In our case this platform is capable to integrate DLMS / COSEM compliant energy meters with LoRaWAN, where a study of LoRaWAN performance, when transporting energy metering packets, in a real-world environment is performed. The LoRaWAN technology has been chosen as a low-cost, long-range, and reliable last-mile solution for smart energy metering in urban areas scenario where a short-range solution may not be the optimum one, however, DLMS / COSEM was chosen since it is the world standard application protocol for smart energy metering, control, and management and it is getting widely accepted in Europe and US. The combination of these two protocols presents significant challenges such as designing an interoperable module that can be easily integrated into the existing infrastructure and is able to meet both LoRaWAN and DLMS/ COSEM transmission requirements in terms of transmission time and packet size. In addition, there are always some security challenges to consider, since cyber-attacks can not only threaten the consumer's privacy but they can even lead to a compromised system with direct impact on the safety of individuals and the activities of society. Therefore, we propose an approach based on combining Secure Element and Blockchain technologies to provide an end to end IoT secure platform. Secure Element has been used to provide IoT nodes with some computational power where Blockchain has been used to enhance integrity, transparency, and security it is used to certify the transmitted energy metering data and to provide these data to Distributed Applications (DApp). In this way, producers and consumers will be able to trade energy (especially from distributed renewable energy sources) over the existing infrastructure, using Blockchain technology, thus leading to the democratization of the energy market.

Keywords: IoT, LPWAN, LoRa, LoRaWAN, DLMS/COSEM, Renewable Energy Resources, Energy Smart Metering, Smart Grid, Secure Element Cyber-Security, Blockchain.

Résumé en Français

Résumé

Avec la croissance mondiale de la consommation d'électricité et l'utilisation de combustibles fossiles pour produire de l'électricité ayant conduit au réchauffement climatique, l'intégration des énergies renouvelables distribuées et des ressources énergétiques propres devient obligatoire et indispensable à très court terme. Pour intégrer ces ressources, les gouvernements se sont concentrés sur la conversion du réseau électrique traditionnel afin qu'il soit plus intelligent et plus efficace. La notion même de réseau intelligent regroupée sous le nom de smart Grid (SG) est une amélioration des réseaux existants utilisant les technologies de l'information et de la communication (ICT) pour améliorer l'efficacité, la durabilité et la fiabilité des réseaux électriques. SG en tant que système cyber-physique recouvre le réseau traditionnel avec un réseau IoT (Internet des objets) qui se compose de compteurs intelligents (SM) pour contribuer à la gestion, au contrôle et à la surveillance des paramètres de consommation en temps quasi réel.

Cependant, les systèmes cyber-physiques deviennent de plus en plus difficiles à surveiller et à gérer avec des architectures centralisées. D'énormes plates-formes ont été conçues pour gérer les énormes quantités de données produites par les appareils IoT, tandis que d'autres platesformes tentent de gérer les problèmes de fonctionnement et de gestion du réseau, des commandes de transfert aux mises à jour du firmware.

Par conséquent, une passerelle de réseau domestique qui facilitera l'intégration des ressources énergétiques locales dans le réseau intelligent doit être développée avec les technologies IoT et de réseau de capteurs sans fil (WSN) intégrées nécessaires, en tenant compte des problèmes de sécurité et d'évolutivité au sein dedans le domaine du comptage du réseau et de la surveillance de la qualité de l'énergie, de la gestion de la charge et de l'automatisation des bâtiments, de l'optimisation de la consommation d'énergie et du négoce d'énergie en temps réel.

Pour chaque plate-forme technologique et les cas d'utilisation associés, différents protocoles et dispositifs physiques sont impliqués, avec des exigences et des capacités différentes. Alors la participation et l’intégration d’un dispositif physique de réseau domestique (Home Aera Network, HAN) avec des rôles, des fonctionnalités et des restrictions/spécifications différentes est

utile. Par exemple, au lieu d'avoir différents appareils, la même passerelle de compteur intelligent devrait se comporter différemment pour l'opérateur de réseau et le consommateur, un agrégateur de données ou une plateforme de trading. Cela nécessite un environnement extrêmement sécurisé mais flexible.

La combinaison des technologies des registres distribués avec des agents intelligents et le traitement des données à la périphérie du réseau peut conduire à une plate-forme efficace qui peut s'adapter avec succès aux défis ci-dessus. À l'aide de projets open-source Distributed Ledger Technology (DLT) tels que Hyperledger (open source Blockchain et outils associés), une architecture de plate-forme de passerelle multi-rôle sera développée, conçue pour fonctionner à la périphérie, communiquant avec différents réseaux d'appareils locaux et services centraux, afin de répondre à des différents besoins et objectifs, en toute sécurité et de garantir que la partie appropriée de la fonctionnalité et des informations est fournie à chaque partenaire de communication

Méthodologie

Ma thèse rédigée en anglais est intitulée "Distributed renewable energy resources enablement based on a secure and versatile electricity trading architecture ». Nous avons traduit le titre en français par " Développement d'une architecture sécurisée et polyvalente d'échange d'électricité d'origine renouvelable dans une approche smart-grid ".

Bien que l'accent ait été mis sur la réalisation et le test d'une telle plateforme open-source de passerelle intelligente de comptage d'énergie, ce travail peut être divisé en deux parties. La première partie est consacrée à l'étude et à la définition des technologies à l'origine de l'évolution du réseau énergétique conventionnel, en particulier l'Advanced Metering Infrastructure (AMI) et les technologies de communication pour la transmission des données énergétiques entre les différents réseaux au sein de l'AMI, où nous nous concentrons principalement sur le Neighborhood Area Network (NAN). La deuxième phase est dédiée à l'étude des performances de LoRaWAN dans la transmission des données énergétiques au concentrateur, en développant un prototype de passerelle open-source où le secteur de l'énergie libanais a été considéré comme étude de cas spécifique pour l’application de nos modèles. Le prototype développé est compatible et adapté au réseau énergétique traditionnel libanais où le gouvernement compte toujours sur les ressources humaines pour collecter les données de consommation d'énergie des utilisateurs. Ensuite, ce système a été développé et testé pour réaliser une plate-forme de télémétrie open-source et à faible coût capable d'intégrer des compteurs d'énergie conformes aux standards DLMS / COSEM sur LoRa. DLMS/COSEM ou IEC 62056, (pour Device Language Message Specification/ Companion Specification for Energy Metering), est la principale norme mondiale pour le comptage, le contrôle et la gestion intelligent de l'énergie qui est accepté et généralisé en Europe et aux États-Unis.

Enfin puisque les énergies renouvelables se développent rapidement dans le cadre de la révolution énergétique en cours, la structure des systèmes énergétiques devient progressivement de plus en plus décentralisée. Avec cette décentralisation, de nouveaux acteurs, tels que les prosommateurs, qui sont les utilisateurs du réseau de distribution pour la distribution de l’énergie qu’ils produisent. Ces prosommateurs à faible capacité d'énergie produite ne peuvent pas participer au marché de l'énergie à grande échelle, mais pourraient organiser un commerce d'énergie local P2P sans l'intervention d'aucune autorité ou d'un tiers. Afin de fournir un commerce d'énergie P2P sécurisé efficace, la mise en œuvre du marché local de l'énergie (LEM) nécessite des technologies d'information et de communication originales et sécurisées, comme la blockchain et la Smart Meter Gateway (SMGW) qui aident le système énergétique à devenir plus décentralisé, intelligent et interconnecté. Au niveau européen, les fonctionnalités allemandes de la passerelle des compteurs intelligents ont été prises comme architecture de référence de la passerelle multiprotocole pour le commerce de l'énergie.

Contributions de la thèse

D’un point de vue macroscopique, la principale contribution de cette thèse est la conceptualisation et le test d'une passerelle sécurisée des compteurs intelligents pour fournir un système d'échange d'énergie P2P sécurisé. Cette passerelle proposée est perçue comme ayant les caractéristiques ci-dessous

- Holistique et agile.
- Système open-source qui peut être utilisé et appliqué dans différentes applications.
- Système modulaire et évolutif.
- Sécurité assurée par un élément sécurisé intégré au système.
- Immuabilité basée sur l’intégration d’une base de données distribuée blockchain.
- Système sécurisé avec non-répudiation.

Pour y parvenir, le premier objectif est de donner une compréhension globale de la structure du réseau intelligent (Smart Grid), y compris les différentes parties impliquées dans la communication et ses applications standard. Il fournit une approche holistique des différentes technologies utilisées dans le lancement du marché de l'énergie Peer to Peer (P2P), telles que Smart Grid, Smart Meter, Low Power Wide Area Networks (LPWAN), AMI (Advance metering infrastructure), systèmes IoT, et les dispositifs de bord de réseau, qui s'appuient sur une meilleure compréhension de l'infrastructure de mesure avancée (AMI) qui est à l'origine de l'évolution du réseau énergétique conventionnel et sur le développement d'une bonne connaissance de l'Internet de l'énergie, du réseau intelligent et des ressources énergétiques distribuées (DER) en particulier les protocoles utilisés pour les technologies de communication et de mise en réseau dans les Smart Grids. De plus, une étude des technologies des registres distribués open source et leur application dans le cadre de l'internet de l'énergie est réalisée.

Le second objectif est de développer et implémenter un prototype de passerelle (Gateway), testé en réalisant des expérimentations liées aux problématiques de mise à l'échelle en fonction du nombre de Gateways supportés, de sécurité du firmware de la Gateway, de confiance et d'intégrité des messages échangés en utilisant la technologie Blockchain pour améliorer l'intégrité et la sécurité. Cette technologie est utilisée pour certifier les données de comptage d'énergie transmises et pour fournir ces données aux Applications Distribuées (DApp). De cette façon, les producteurs et les consommateurs pourront échanger de l'énergie (en particulier à partir de sources d'énergie renouvelables distribuées) sur l'infrastructure existante. Le système conceptualisé a comme architecture de référence le SMGW allemand et intègre deux technologies principales Secure Element et Blockchain. Cette approche combinatoire surmonte le risque d'utiliser une technologie unique. Ensuite, nous avons appliqué notre système au domaine de l'énergie afin de permettre un échange d'énergie P2P sécurisé.

En combinant ces deux technologies sous un même système, nous sommes en mesure de répondre à deux préoccupations de sécurité: Le premier problème est de sécuriser les données à la source de génération (racine de confiance). Puisque les appareils distants manquent de ressources pour valider les données, l'intégration du Secure Element et de la périphérie fournira au nœud un mécanisme de signature qui vérifiera l'origine des données avant d'être publiées sur la blockchain.

Deuxièmement, en utilisant le Secure Element, nous fournissons l'immuabilité des données car les données ne seront pas alternées ou modifiées par un pirate informatique intermédiaire avant d'être publiées sur la blockchain.

Organisation du manuscrit de la thèse

Cette thèse est composée de cinq chapitres qui sont résumés ci-dessous:

Le chapitre 1 vise à décrire l'évolution du réseau énergétique conventionnel en définissant et en décrivant le système Advanced Metering Infrastructure (AMI). Nous abordons les technologies de communication en usage, en plus d'une étude bibliographique rapide qui couvrira les vulnérabilités de cybersécurité des compteurs intelligents basés sur les technologies de communication sans fil LPWAN où nous avons montré certaines failles de sécurité liées au système SG, pouvant compromettre l'ensemble du système et menacer la vie privée de l'utilisateur. Par conséquent, nous avons proposé quelques meilleures pratiques de sécurité AMI, qui peuvent sécuriser le système, seront répertoriées à la fin.

Le chapitre 2 donne un aperçu des progrès actuels et à venir de l'IoE, des cas d'utilisation, des applications et des plans d'action associés en Europe. Un accent particulier sur l'introduction de l'état actuel de l'IoE dans des pays européens comme l'Allemagne et la Grèce. Le système allemand a été présenté et discuté en détail car il a été utilisé comme architecture de référence de notre passerelle de comptage d'énergie développée.

Les chapitres 3 et 4 présentent la conception, la réalisation d'une passerelle énergétique open-source, ainsi que les contraintes et défis surmontés auxquels nous avons été confrontés en termes de conception et de modularité. Le prototype conçu sera présenté en détail, en plus la mise en œuvre et les résultats des tests seront expliqués et discutés. Ces deux chapitres proposent la conception et le déploiement d'un système open-source, low-cost et modulaire basé sur la technologie de télécommunication LoRa pour les applications de comptage d'énergie.

Dans le chapitre 3, la solution a été conçue et proposée pour le marché libanais comme une solution importante pour accéder aux pannes d'électricité en déployant une infrastructure de comptage d'énergie en temps quasi réel. La conception a été déployée et testée sur site en situation réelle, dans une application expérimentale de comptage d'énergie, où les valeurs mesurées ont été publiées sur un serveur cloud, permettant d'exécuter des analyses et d'être accessibles simultanément par les opérateurs du secteur de l'énergie et les propriétaires de compteurs intelligents. Ces valeurs peuvent être consultées, traitées et présentées à l'aide d'une multitude d'outils permettant le déploiement de services tiers précieux tels que la mise en œuvre de centrales électriques virtuelles pour la réduction de l'énergie et l'introduction de technologies de grand livre distribué pour l'énergie peer-to-peer commerce.

Le chapitre 4 présente les avantages de l'adoption de solutions IoT à faible coût et des normes de protocole de communication Smart Metering ciblant la rénovation des réseaux électriques existants vers des réseaux intelligents avec des capacités d'échange d'électricité peer to peer. Dans ce cadre, nous proposons une architecture de réseau intelligent basée sur la norme de communication de comptage d'énergie DLMS/COSEM et les technologies de communication LPWAN, tandis qu'une couche Blockchain permet l'intégrité des données de comptage intelligent pour le commerce de l'électricité.

Le chapitre 5 représente la passerelle énergétique développée comme cas d'utilisation pour le commerce d'énergie P2P de quartier. Notre hypothèse est que la passerelle développée permettra le marché local de l'énergie sans l'intervention des services publics où les petits prosommateurs peuvent participer ainsi un bon investissement des ressources énergétiques renouvelables. Ce manuscrit qui avait commencé par une introduction se termine par une conclusion générale sur cette étude et rappelant les résultats originaux obtenus à laquelle se rajoute une partie, perspectives que ce travail permet d’envisager. Des listes d’acronymes et de références bibliographiques sur lequel ce travail fait références sont également présentes dans ce manuscrit.

Table of contents

Acronyms

ABP	Activation by Personalization
ADC	Analog to Digital Converter
AMI	Advanced Metering Infrastructure
AMR	Automated Meter Reading
ANSI	American National Standards Institute
APDU	Application Packet Data Unit
BMS	Building Management systems
BPSK	Binary Phase-Shift Keying
CLS	Controllable Local Systems
CRC	Cyclic Redundancy Check
DAC	Digital to Analog Converter
DApp	Distributed Applications
DCU	Data Concentrator Units
DERs	Distributed Energy Resources
DG	Distributed Generation
DLT	Distributed Ledger Technology
DMS	Data Management System
DoS	Denial-of-Service
DR	Data Rate
DS	Distributed Storage
DSSS	Direct Sequence Spread Spectrum
ECDH	Elliptic Curve Diffie Hellman
EMP	External Market Participants
GFSK	Gaussian Frequency-Shift Keying
HAN	Home Area Network
HEMS	Home Energy Management System
HMAC	Hashed Message Authentication Code
ICT	Information and Communication Systems
IEA	International Energy Agency
IEC	International Electro-Technical Commission
IETF	Internet Engineering Taskforce
iMSys	Intelligent Metering Systems
IoE	Internet of Energy
IoT	Internet of Things
ISM	Industrial Scientific and Medical
LEM	Local Energy Market

LMN	Logical Metrological network
LoRa	Long Range Radio
LoRaWAN	Long Range Wide Area Network
LPWAN	Low Power Wide Area Networks
LV	Low-Voltage
M2M	Machine to Machine
MAC	Message Authentication Code
MCU	Microcontroller Unit
MDMS	Meter Data Management System
MIC	Message Integrity Codes
NAN	Neighbor Area Network
NB-IoT	Narrowband-Internet of Things
NIST	National Institute of Standards and Technology
OBIS	Object Identification System
OTA	Over the Air
OTAA	Over-the-Air Activation
P2P	Peer to Peer
PLC	Power Line Carrier
PMU	Phase Measurement Units
QoS	Quality of Service
RES	Renewable Energy Resources
RF	Radio Frequency
SF	Spreading Factor
SG	Smart Grid
SGAM	Smart Grid Architecture Model
SM	Smart Meter
SMGA	Smart Meter Gateway administrator
SMGW	Smart Meter Gateway
SN	Sequence Number
SNR	Signal-to-Noise Ratio
WAN	Wide Area Network
WSN	Wireless Sensor Network

List of Figures

General Introduction

General Introduction

With the global electricity consumption growth and the use of fossil fuels to generate electricity has led to global warming, therefore the integration of distributed renewables and clean energy resources becomes a must. To integrate these resources governments have focused on converting the traditional power grid to be smarter and more efficient. Smart Grid (SG) is an enhancement of existing grids using Information and Communication Technologies (ICT) to improve the efficiency, sustainability, and reliability of power grids. SG as a cyber-physical system overlays the traditional grid with an IoT (Internet of Things) network that consists of Smart Meters (SM) to contribute to the management, control, and monitoring of consumption parameters in near real-time. SG implementation is based on introducing a chain of technologies that include Smart sensors, IT systems, Smart Meters (SM), and communication networks

However cyber physical systems are becoming increasingly difficult to monitor and manage with centralized architectures. Huge platforms have been built to handle with the huge amounts of data produced by IoT devices, while other platforms attempt to handle operational and network management issues, from transfer commands to firmware updates.

Therefore, a Home Area Network gateway that will facilitate the integration of the local energy resources into the smart-grid, has to be developed with the necessary integrated IoT and wireless sensor network (WSN) technologies integrated, taking into account security and scalability issues within the scope of grid metering and power quality monitoring, load management and building automation, optimization of energy consumption and real-time energy trading.

For each technological platform and related use cases, different protocols and physical devices are involved, with different requirements and capabilities. But a useful home area network (HAN) physical device should participate in many of them, with different roles, features and restrictions/specifications. For example, instead of having different devices, the same smart meter gateway should behave differently for the network operator, the consumer, a data aggregator, or a trading platform. This requires an extremely secure but flexible environment.

The combination of Distributed Ledger Technologies with autonomous agents and edge computing can lead to an effective platform that can successfully adapt to the above challenges. Using open-source Distributed Ledger Technology (DLT) projects such as Hyperledger-based (open source blockchains and related tools) a multi-role Gateway platform architecture will be developed, designed to operate at the edge, communicating with different networks of local devices and central services, in order to fulfill different needs and purposes, with safety and to ensure that the appropriate part of the functionality and information is provided to each communication partner

Methodology

My thesis work is titled "distributed renewable energy resources enablement based on a secure and versatile electricity trading architecture". Although the focus has been on realization and testing of such an open-source platform smart energy metering gateway, this work can be divided into two parts. The first part is dedicated to study and define the technologies behind the evolution of the conventional energy grid, in particularity the Advanced Metering Infrastructure (AMI) and communications technologies for energy data transmission between different networks within the AMI, where we mainly focus on the Neighbor Area Network (NAN). The second phase is dedicated for studying the performance of LoRaWAN in transmitting the energy data to the concentrator, by developing an open-source gateway prototype where the Lebanese energy sector was taking as a case study. The developed prototype was compatible and adequate to the Lebanese traditional energy grid where the government still relies on human resources to collect user's energy consumption data. Then this system was developed and tested to realize an open-source, low-cost telemetry platform that is capable to integrate DLMS / COSEM compliant energy meters over LoRaWAN; where DLMS / COSEM is the global standard application protocol for smart energy metering, control, and management which is getting widely accepted in Europe and US. T.

Finally since renewable energy are rapidly growing as part of energy revolution. Energy systems structure is becoming progressively decentralized. With this decentralization new players, such prosumers with low produced energy capacity who cannot participate in energy market, could organize a P2P local energy trading without the intervention of any authority or third party and in order to deliver an effective secure P2P energy trading, the implementation of Local Energy Market (LEM) requires original and secure information and communication technology, like

Blockchain and Smart Meter Gateway (SMGW) which help the energy system to become more decentralized, smart and interconnected. However the German smart meter gateway functionalities were taken as reference architecture of the multi-protocol Gateway for Energy trading.

Thesis' Contributions

On a high level, the main contribution of this these is the conceptualization and testing of a secure smart meter gateway to provide a secure P2P energy trading system. These proposed gateway is perceived to have the below characteristics

- Holistic and agile.
- It is an open-source system that can be used and applied in different filled.
- Modular and scalable.
- Provides security by integrating secure element.
- Provides immutability by integrating Blockchain distributed database.
- Secure system with non-repudiation.

To achieve this, the first goal is to give an overall understanding of the Smart Grid structure, including the different communication involved parties and its standard applications. It provides a holistic approach of different technologies that are used in the Peer to Peer (P2P) energy market launching, such as Smart Grid, Smart Meter, Low Power Wide Area Networks (LPWAN), AMI (Advance metering infrastructure), IoT systems, and grid edge devices, which based on obtaining a better understanding of the Advanced Metering Infrastructure (AMI) that is behind the evolution of the conventional Energy Grid and developing a good knowledge of Energy Internet, Smart Grid and Distributed Energy Resources (DERs) in particular the used protocols for communication and networking technologies in Smart Grids. Moreover, a study of an open source Distributed Ledger Technologies and Applications under the scope of the energy internet is done, in addition to Cyber Physical Systems and simulation tools for the development of a versatile and secure Gateway for sensing and actuation targeting to the integration of DERs in contemporary Smart Grids were an important part.

The second objective is to develop and implement a prototype Gateway platform, tested by realizing experiments related to the issues of scaling according to the number of supported

Gateways, security of the Gateway firmware, trust and integrity of the exchanged messages by using Blockchain technology to enhance integrity, transparency, and security. This technology is used to certify the transmitted energy metering data and to provide these data to Distributed Applications (DApp). This way, producers and consumers will be able to exchange energy (especially from distributed renewable energy sources) over the existing infrastructure. The conceptualized system has as a reference architecture the German SMGW and integrates two main technologies Secure Element and Blockchain. This combinational approach overcome the risk of using any technology alone. Then we applied our system to energy field to enable secure P2P energy trading.

By combining these two technologies under one system, we are able to answer two security concerns:

The first problem is to secure data at the source of generation (root of trust) .since the remote devices lack the resources to validate data, the integration of secure element and the edge will provide the node with a signature mechanism that will ascertain the origin of becoming data before being published on Blockchain.

Secondly by using the secure element we provide data immutability because data will not be alternate or modified by any intermediary hacker before being published to blockchain.

Thesis Organization

The manuscript of this thesis is composed of five chapters which are summarized below:

Chapter 1 is intended to describe the evolution of the conventional energy grid by defining and describing the Advanced Metering Infrastructure (AMI) system. We approach the communication technologies in use, in addition to a quick bibliographical study that will cover the cyber security vulnerabilities of smart metering based on LPWAN wireless communication technologies where we showed some security breaches related to the SG system, can compromise the whole system and threat the user privacy. Therefore, we came out with some AMI security best practices, that can secure the system, will be listed at the end.

Chapter 2 gives an overview of the current and upcoming IoE advancements, use cases, applications and related plans of action in Europe was provided. A particular focus, on introducing IoE current state in Europe countries like Germany and Greece. The German system was presented and discussed in details since it was used as reference architecture of our developed energy metering gateway.

Chapters 3 and 4 present the designing, realization of an open-source energy gateway, and the overcome constraint and challenges that we faced in terms of design, and modularity. The designed prototype will be presented in details, in addition the implementation and testing results will be explained and discussed. These two chapters propose the design and deployment of an open-source, low-cost, and modular system based on LoRa telecommunication technology for energy metering applications.

In chapter 3 the solution was designed and proposed for the Lebanese market as an important solution for accessing the electricity outages by deploying a near real-time energy metering infrastructure. The design was deployed and tested in an experimental energy metering application, where the measured values were published to a cloud server, allowing for running analytics and be accessible from the Energy sector operators and the smart meter owners simultaneously. These values can be accessed, processed, and presented using a multitude set of tools enabling the deployment of third-party valuable services like the implementation of Virtual Power Plants for Energy curtailment, and the introduction of Distributed Ledger Technologies for peer-to-peer energy trading.

Chapter 4 presents the benefits of adopting low-cost IoT solutions and Smart Metering communication protocol standards targeting the renovation of existing electricity Grids to Smart Grids with peer-to-peer electricity exchange capabilities. Towards this scope, we propose a Smart Grid Architecture based on the DLMS/COSEM energy-metering communication standard and LPWAN communication technologies, while a Blockchain layer enables the smart-metering data integrity for electricity trading.

Chapter 5 represents the developed energy gateway as a use case for neighborhood P2P energy trading. Our assumption is that the developed gateway will enable the local energy market without the intervention of the utilities where small prosumers can participate thus a good investment of Renewable Energy Resources (RES).

The first part of each chapter of this manuscript will present a literature review of each technology, how it was used in our case in addition to a description of the measures, an initial analyzes of the results and a discussion of the observed results.

Finally, this monograph ends with a general conclusion. This conclusion recalls the different technologies and procedures used, the various prototype designing obstacles that we have removed and summarizes the fundamental results obtained during these years of thesis. The future work is eventually considered in this last part.

Chapter 1 : Smart Grid Technological Background, Introduction to Advance Metering Infrastructure.

1. 1 Introduction

With the global electricity consumption growth and using fossil fuels to generate electricity led to global warming. The integration of distributed renewables and clean energy resources becomes a must. To integrate these resources governments have focused on converting the traditional power grid to be smarter and more efficient. Smart Grid (SG) is an enhancement of existing grids using Information and Communication Technologies (ICT) to improve the efficiency, sustainability, and reliability of power grids. SG as a cyber-physical system overlays the traditional grid with an IoT (Internet of Things) network that consists of Smart Meters (SM) to contribute to the management, control, and monitoring of consumption parameters in near real-time. SG implementation is based on introducing a chain of technologies that include Smart sensors, IT systems, Smart Meters (SM), and communication networks [1]. For example, smart metering, which is a basic function in smart grids, permits the provider to have an overview of the consumer's power consumption in real-time and to modulate the amount of generated power to satisfy his energy needs without any unnecessary waste. Since smart metering is based on embedded systems technologies and connected to a network it become vulnerable to cyber-attacks, despite all its advantages. Smart meters are distributed everywhere. Both the smart meter and the transmission medium are physically exposed to hackers. Therefore, the data collected by meters are exposed and could be stolen, intercepted, altered or the meter itself could be compromised, with a wide variety of negative side effect to the whole network infrastructure. Hence, to protect the privacy and the integrity of these readings it is important to emphasize the crucial role of security and to consider it from the beginning of the SG design and throughout the whole lifecycle of system implementation and evolution.

Moreover, while the majority of meters are installed in clustered areas, there are still some nodes in difficult to reach places far away from any available cluster. Although these nodes are not many in quantity, studies show that 1% of these nodes can represent 50% of the total operational cost of the network. Therefore, up to 50% of the unnecessary cost can be saved by the integration of Low Power Wide Area Networks (LPWAN) wireless communication system to reach these 1% nodes. Also, LPWANs in perfectly suitable for the IoT applications because they effectively meet the connectivity requirements in large area, ideal for connecting devices such as sensors for their use in monitoring variables. With the adoption of LPWAN technologies for smart metering, it is expected that the number of SM connected will reach 153.3 million out of 1.2 billion smart meters in total, that will be installed over the next ten years—a small but growing share of 12.7%—according to a new study published [2]. So, it is obvious that LPWAN is reserving its place in the smart metering systems in the upcoming years with the freedom and flexibility that wireless communication technologies provide.

This Chapter focuses on defining a detailed approach of the Advanced Metering Infrastructure (AMI) system. It examines the communication requirements and discusses the communication architecture of the AMI by studying the speciation and security vulnerabilities of different used short-range wireless technologies and LPWAN which their integration will affect the smart metering infrastructure followed by an overview of a smart metering system, specifically Dutch smart metering system since it was the reference of our developed prototype, and the different existing communication networks (focusing on wireless technologies) that are used in the last mile of a smart metering infrastructure and their security basics. A comparison of the different security vulnerabilities of the wireless communication technologies based on the existing literature is presented. This chapter ends with a list of the suggested security improvements released for AMI and our proposed recommendations.

1. 2 Conventional Power Grids

Over the years, the world's energy needs have been satisfied by the electrical power systems, where these systems rely substantially on many remote power plants that operate from conventional sources like natural gas, and fossil fuels. high-voltage for the transmission systems and low-voltage at distribution system level to transfer the energy to the final consumption side [3]. Conventional power grids are based on a centralized management system that includes a group of actors who are responsible for managing the power grid and its operations for example they control and schedule the power production and they are responsible of a reliable energy delivery to the consumer end. These actors are represented by the generators, utilities, transmission networks, energy market, power supply company and distribution systems operators. The technical parameters and functions of each actor are defined and decided by the governance structure of the power grid. Therefore, the market rules, the structures regularity and the predefined policies impose an impact on the role and the operation of each actor and this what characterized the majority of the worldwide electrical power grid.

1. 3 Rise of RES and their Integration Challenges

A few years ago, due to environmental pollution and energy crisis around the world, the energy policy makers took serious action, against the rising challenges, and began changing the power systems. The integration and the investment of the RES was and still the first solution. Different strategies, programs and scenarios have been initiated to reduce the dependences on fossil fuels [4]. Renewable energy resources are being introduced to the energy market and are reserving an important place in the energy market. Good to mention that lately worldwide governments are funding programs to encourage consumers to install renewables on their properties [5].

Furthermore, there has been a remarkable drop in the price of renewable energy equipment. As a consequence, an inflation can be observed in the sale and production of RES equipment's as shown in Figure 1-1: Renewable Energy Capacity Growth [6] many consumers are now a part of small-scale renewable energy production, by installing different RES like solar panels, micro wind turbine and fuel cells.

These participants are now considered as prosumers, in fact they are producer and consumer at the same time since they produce energy by their RES but they still rely on the conventional power grid.

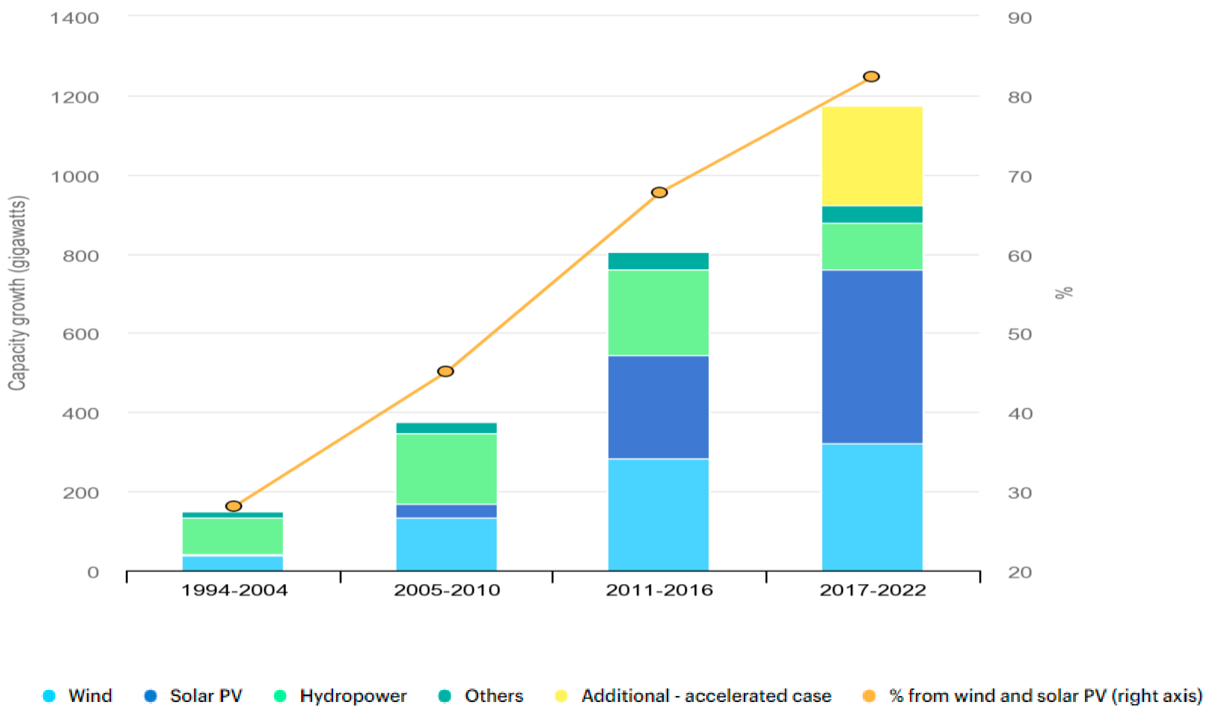


Figure 1-1: Renewable Energy Capacity Growth [6]

According to the International Energy Agency (IEA), it is expected that 30% of the world power production will be generated from the RES by the end of 2022 [6] . Although, the capacity of energy produced by the RES is growing and meeting the expected agenda for building a low-carbon electricity sector, it also faces challenges presented by the existing electricity system technical settings. Since renewable energy technologies are highly dependent on climate-related factors including sunlight, wind speed and water availability. Also, it is hard for the current grid capacity to tolerate the pressure of expanding bidirectional unsteady flows of energy. Furthermore, the current governance structure needs to be updated and enhanced to integrate new players, known as prosumers, into the energy market. In addition, the insertion of intelligent and smart devices, the Electrical Vehicule (EV's) is an evident sign of immense need of energy which will stress out the need of a better RES management. In this context, the main challenges that a related to the enhancement and development of the energy power system to integrate the RES are the following:

1. Centralized management system: to deal with fluctuation energy demand the system operators control the power supply, with the RES integration new fluctuating energy supplies are added. The RES variety makes the system management more sophisticated and complex.

2. Real-time data: Since the bidirectional communication between the users and operators is therefore required a real time data on the actual grid state, operations, particularly consumption and production at the end user level (distribution level), to control the flexibility of demand.
3. Unidirectional power transmission: The current system is still vulnerable to an unstable bidirectional RES flow that stresses the grid capacity.
4. Governance framework: it is still necessary to work on and improve a clear legal framework in order to adjust the new roles played by prosumers (transforming a consumer into a prosumer).

As a result, in order to address the challenges mentioned above a new generation of power grid has been introduced the Smart Grid (SG). Smart Grid is equipped with Internet of things (IoT) devices, such as wireless sensor, Smart meters for advanced metering infrastructure, where these devices have enabled the bidirectional communication between components and will lead to a dynamic infrastructure capable of managing the energy demand response Figure 1-2 shows the power grid evolution.

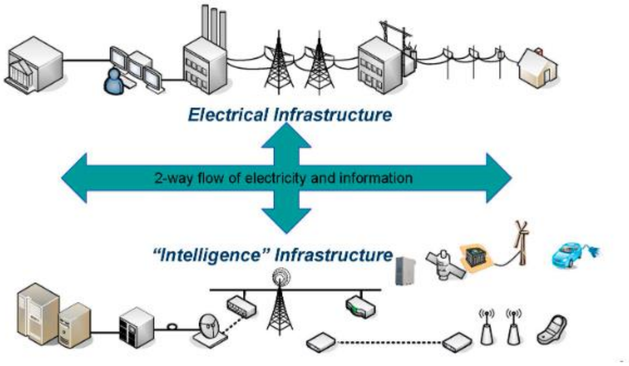

Electrical Infrastructure
2-way flow of electricity and information
"Intelligence" Infrastructure

Figure 1-2: Power Grid Evolution.

1. 4 Smart Grids

The next generation of the traditional electricity grid is the Smart Grid (SG), it is considered a revolution of the existing conventional power grid. It will be a solution to improve the electrical energy system not only by integrating Renewable Energy Resources (RES), but also Distributed

Generation (DG) and Distributed Storage (DS). This evolution, which is based on the introduction of ICT (Information and Communication Technologies), will improve the efficiency, sustainability, and reliability of power grids. Smart Grid aims to solve different existing problems in power delivery, respond to climate change, improve energy efficiency, and open a new direction in electricity markets (like Peer-to-Peer P2P energy trading). The two-way communication enabled between the smart grid components and the utility, which offers many advantages such as demand management and early blackouts detection, combined with the information, communication, control, computer and wireless sensor technologies make the power grid smarter. The Smart Grid Architecture Model (SGAM) framework is presents in Figure 1-3

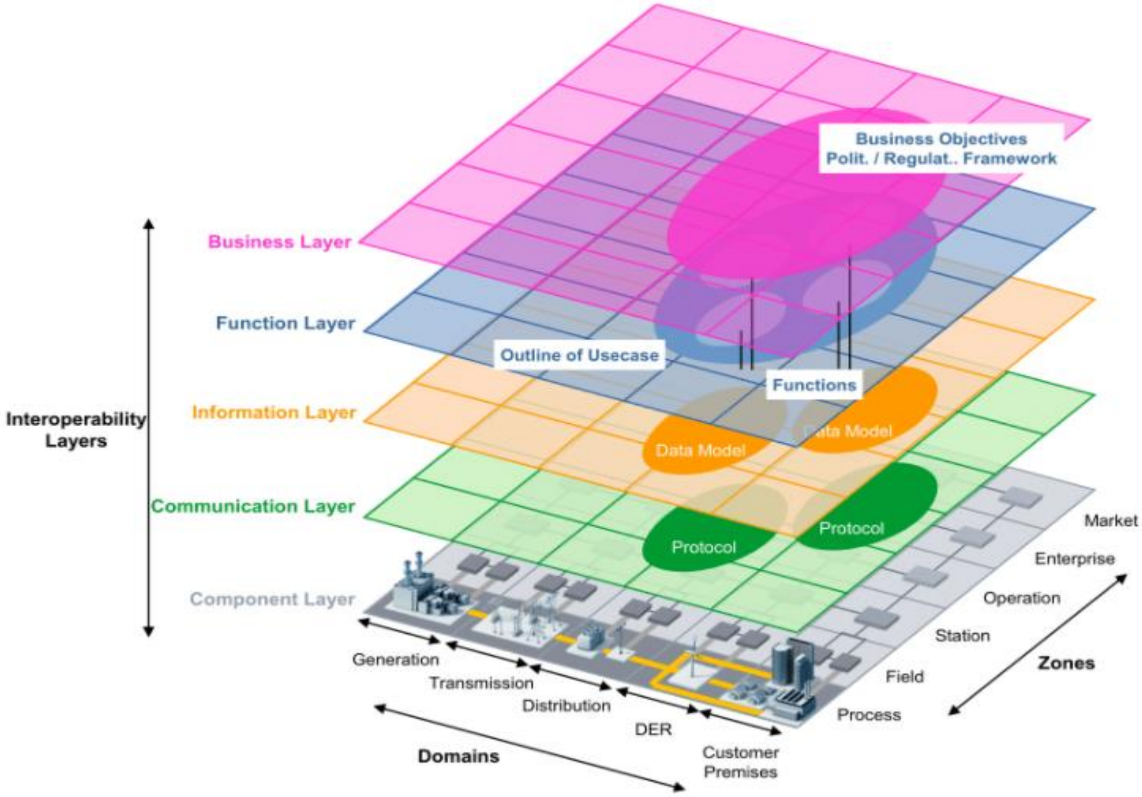


Figure 1-3: Smart Grid Architecture Model (SGAM) framework [7].

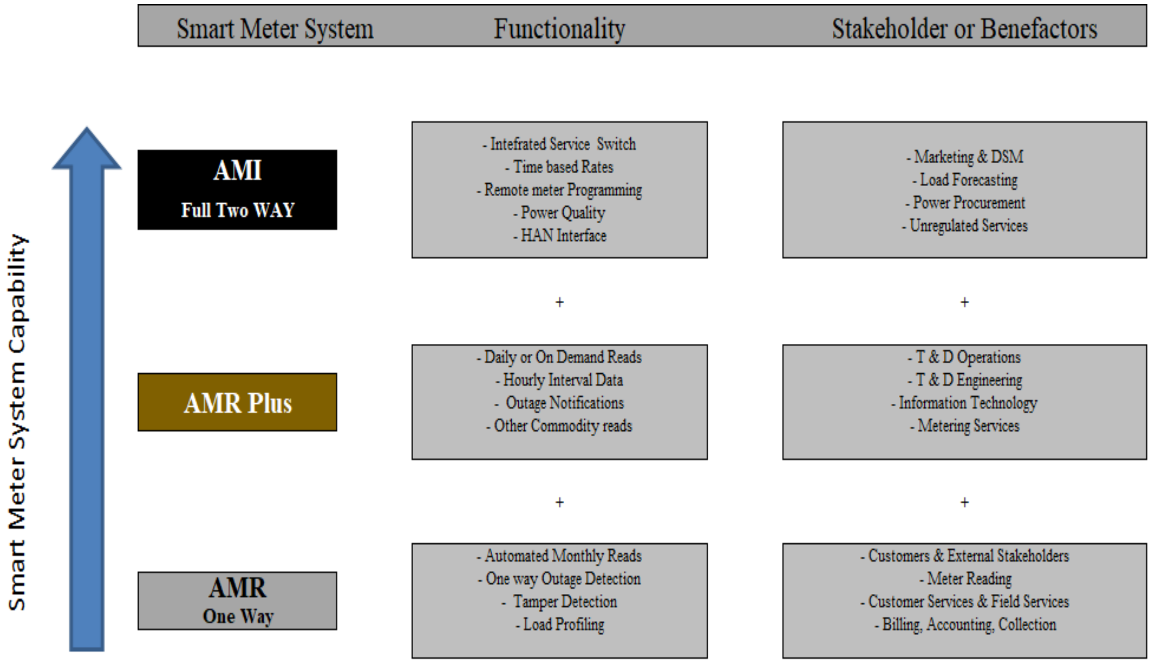
The SGAM defines the reference model of the SG, it is established by merging the concept of interoperability of layers with the SG plane. It represents the hierarchies of power system equipment (domains) and the information management systems (zones) that control them. The Combination of these two dimensions produces a representation between the control systems and the processes that they control, known as the SGAM Smart Grid Plane.

Based on Figure 1-3 the SGAM consists of five interoperability layers representing business objective and processes, functions, information exchange and communication protocols, and components. It is important to note that in addition to the relation that exists between the components of the same layer, there is an interrelation between the components of different layers. For example, the realization of a business process (object of the business layer) is carried out by a function (object of the function layer) and this function is executed by a component (object of the component layer). However, the function execution is based on a component that supports a data model and a communication protocol that are information and communication layer objects respectively [8]. In our case we will be focusing on the component and communication layer.

1. 5 Smart Metering System: Advance Metering Infrastructure (AMI)

1. 5. 1 AMI Evolution

The latest infrastructure investments focus on the metering part, with the Automated Meter Reading (AMR) as the first trial, which provides utilities with remote basic information about each consumer-user energy consumption[9]. But the AMR system was restricted to a remote reading and cannot provide utilities with additional information or data due to the support of a one-way communication system. The direct implication of the Smart Grid to have an electric model able to manage different generation and storage devices in an efficient and decentralized way and the above mentioned limitation has pushed utilities to move towards Advanced Metering Infrastructure (AMI) and Smart Metering. With AMI, utilities can establish bidirectional communication with the meter, to evaluate the state of the grid, and connect, disconnect, and even configure the electricity service remotely [10]. The latest Smart Metering Systems allow utilities to manage and control the gird on the basis of an improved architecture that works with smart sensors and distributed control technology [11]. Moreover, AMI offers consumers the possibility to access their data through Internet applications to control and manage their energy consumption, pay bills, and to sell their excess of electricity produced from renewables. the AMI allows renewable energy sources on consumers' premises to be integrated into the smart grid [12]. Figure 1-4 shows the evolution from AMR to AMI with lists of stakeholders and benefactors for each step [13].



Smart Meter System	Functionality	Stakeholder or Benefactors
AMI Full Two WAY	- Intefrated Service Switch - Time based Rates - Remote meter Programming - Power Quality - HAN Interface	- Marketing & DSM - Load Forecasting - Power Procurement - Unregulated Services
	+	+
AMR Plus	- Daily or On Demand Reads - Hourly Interval Data - Outage Notifications - Other Commodity reads	- T & D Operations - T & D Engineering - Information Technology - Metering Services
	+	+
AMR One Way	- Automated Monthly Reads - One way Outage Detection - Tamper Detection - Load Profiling	- Customers & External Stakeholders - Meter Reading - Customer Services & Field Services - Billing, Accounting, Collection

Figure 1-4: Evolution of Smart Metering.

1. 5. 2 AMI Components (Smart Meter, Communication Networks, Data Concentrtor and Data Management System)

Smart Meter:

The Smart Meter (SM) is the main component of AMI. SM provides an accurate and remote measurement reading and it communicates with smart home appliances to efficiently manage their energy consumption. These features are made possible by two-way communication and advanced sensors. [14]. A SM has two main communication functions, one to send the data to the utility and receive commands from the grid operator, and the second is to exchange data with the Home Energy Management System (HEMS) [15]. As well, some SMs are equipped with a web-based application that helps consumers to control and monitor their energy use and be aware of their consumption [16]. In general, the main SM characteristics are summarized by energy metering, communication with other smart devices like sensors, and time-based pricing. In addition to the above mentioned features come the security features that include encryption of security data and detection of energy theft [16].

Mainly, a SM is composed of four parts:

- Analog Frond End signal conditioning metering subsystem,
- Communication interfaces,
- Micro Controller Unit (MCU),
- Power system.

The AnalogFrond End signal conditioning metering subsystem integrates the electronics for signal conditioning (amplification, antialiasing filtering, offset compensation) for analog voltage and current signals before digitization. The Microcontroller Unit (MCU) contains an Analog to Digital Converter (ADC) and a Digital to Analog Converter (DAC). The primary role of the MCU's is to control inputs and outputs, to keep track of time stamp operations, preprocess the metering data (digital filtering, harmonics calculations, statistics, encryption, and decryption of measurements), and to store data in RAM, ROM, EEPROM, or Flash memories. As well, the meter activities logs are recorded by the MCU [17]. Communication interfaces are wired or wireless allowing the meter to communicate with the grid and the end user's Home Area Network (HAN). The power subsystem is used to power the electronic components of the smart meter using AC/DC converter. When there is no power from the main line, a battery based backup system is activated automatically. The American National Standards Institute (ANSI) and the International Electro-Technical Commission (IEC) are the two organizations for smart meter standards in the USA and Europe. For example, the IEC 62052 Electricity metering equipment defines the General requirements, tests, and test conditions, the IEC 62052-11 with Part 11 defines the Metering equipment, the IEC 62052-31 with Part 31defines the Product safety requirements and tests, the IEC 62053-22 with Part 22 defines the Static meters for reactive energy (classes 0.2 S and 0.5 S)), and the IEC 62056 Electricity metering defines the Data exchange for meter reading, tariff, and load control, etc.

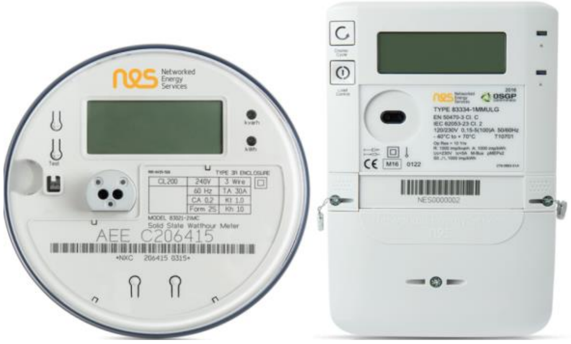


Figure 1-5: Shows examples of ANSI and IEC smart meters [18][19].

Communication Networks

The communication technologies used in SMs are either the wired like a Power Line Carrier (PLC) or the wireless one using radio frequency (RF) transceivers following a plethora of networking technologies like mobile telephony, while recently LPWAN technologies have taken a significant part in this sector. Each of these technologies presents its advantages and disadvantages in an application, for example, the use of wireless communication technologies can be straightforward for hard to reach geographically isolated areas where the infrastructure costs are low compared to wired technologies. However, in the case of wired technologies the interference issues do not exist and the power transmission line can be used for data communications. In a Smart Metering System, the data transmission through power-line communications, wireless communications, cellular technologies or the Internet must be guaranteed in terms of time, quality, and security. The communication systems should cover the security requirements such as:

- Security.
- Bandwidth needed.
- Geographical coverage based on the environment (internal/ external).
- Power quality, with the minimum number of repeaters [20].

As a result, utilities choose the best technology based on technology availability, reliability, operational costs, business needs, and cyber security considerations. In this chapter, only the wireless communications technologies used in the field of Smart Metering will be presented, with their security specifications and vulnerabilities, as the majority of devices used and implemented today in the HAN and NAN are wireless communication nodes.

Data Concentrator

The primary role of the data concentrator is to collect data generated from the SMs in the NAN. In addition, for the management of SMs, the embedded system integrated into modern Data Concentrator Units (DCU) provides a further improvement that manifests itself in the inclusion of an advanced Low-Voltage (LV) supervisor and a Power Line Communication (PLC) controller with network monitoring features.

Data Management System

The Data Management System (DMS) collects and stores the data sent by SMs for processing. In the DMS there are integrated the appropriate subsystems for validation, processing, and editing of the metering data providing the proper exchange of information between different parts of the Smart Metering system [21]. With the evolution of the smart metering system and its capacity in terms of compilers and storage, the DMS has become an advanced system with the ability to make decisions and manage the system in real-time. The data generated by smart metering is very useful for utilities. These data give utilities the ability to go further and work in proactive mode instead of reactive mode. Utilities use the metering data to make a wide range of forecasts and predictive analyses that cover user's consumption predictions, energy availability, and Smart grid stability (power failures).

1. 6 AMI Last-Mile Communication Technologies

To carry out two-way communication the AMI architecture uses different communication networks, each has its own requirements and considerations that were discussed in the previous study and illustrated in Figure 1-6 [22]:

1. Home Area Network (HAN) for energy management at the consumer end.
2. Neighborhood Area Network (NAN) is the last mile for providing the AMI.
3. Wide Area Network (WAN) for communication between all parts of the SG, including control center, renewable energy sources, transmission, and distribution.

The HAN is connected to the WAN via NAN. The NAN is formed of SMs, and the Data collected from SMs will be transmitted to the DCU (Data Concentrator Unit). A high data transmission rate is required at the WAN level therefore, different wireless communication technologies than those used at the HAN/NAN level, are used e.g. WiMAX, 3G/LTE, and micro-wave [23]. Later in this section, the widely used wireless communication technologies adopted by HAN and NAN will be presented.

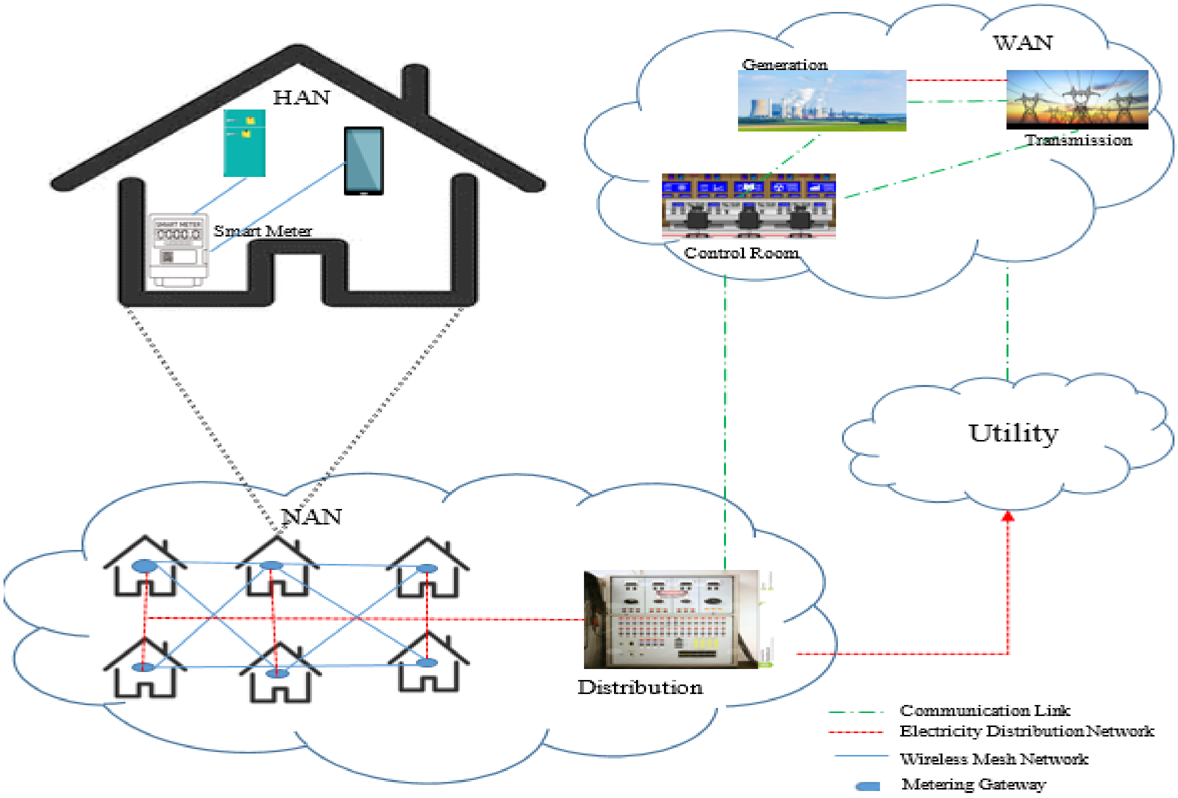


Figure 1-6: Smart Grid Network.

1. 6. 1 HAN Wireless Communication Network

Home Area Network (HAN) is a network in a user's home where all smart appliances and digital devices are connected into a network. The communication between these appliances or devices and the Smart Meter is ensured by the different wireless technologies and protocols available such as ZigBee, Z-wave, Wifi, Bluetooth, 6LoWPAN, wireless M-Bus, and LoRa recently. Data exchanged via wireless communication between the SM and domestic devices consists of information on power consumption and network monitoring. This requires secure Machine to Machine (M2M) communication protocols are needed [24]. The wireless technologies that will be discussed in the HAN area are ZigBee, Wi-Fi, 6LoWPAN, Z-Wave, Wireless M-Bus, and LoRaWAN. For Zigbee and Wi-Fi, different standards which define the first two Layers Physical (PHY) and Medium Access Control (MAC), have been developed by IEEE. For 6LoWPAN it was introduced by IETF (Internet Engineering Taskforce) however for Z-wave it is an appropriate solution.

Zigbee: Zigbee standard is built on the Physical (PHY) layer and Medium Access Control (MAC) sub-layer defined by IEEE 802.15.4 standards, which are the basis of different wireless technologies. The Zigbee protocol stack is composed of four main layers as listed below [25] :

1. The physical layer PHY.
2. The media access layer MAC.
3. Network layer NWK.
4. Application layer APL.

Zigbee adds additional layers to cover the network and application capabilities.

The Physical layer is the physical transmission of the packet's using Direct Sequence Spread Spectrum (DSSS) modulation and demodulation (Radio transmission). The data rate is dependent upon band used, the 2.4 GHz band has a data rate of 250 Kbps per channel, while the 915 MHz band reaches a rate of approximately 40 Kbps per channel and for the 868 MHz band, this rate is down to 20 Kbps. With a point-to-point topology Zigbee coverage can reach up to 10-75m and 30m indoors but with a mesh topology the covered distance is not limited.

The MAC layer, it is used to prevent any collision during frame transmission. Zigbee is based on a wireless mesh network "self-healing network" which means that it is tolerant against Link failures and offers network stability and high scalability. It is composed of three main components:

1. The coordinator, who is responsible for some fundamental functionalities e.g. security management, the definition of frequency in use, session initiation (permits for nodes to join the network).

2. The Router, that is responsible for packets routing between nodes.
3. The End devices, for sending and receiving communication packets with the actual payload.

Zigbee Alliance has developed different standards for different domains like ZigBee Smart Energy, ZigBee Healthcare, and many others. Zigbee is a highly efficient and cost-effective solution [26].

Zigbee Security Basics: Communication security is one of Zigbee's strengths. Zigbee sets 8 security levels. The lower four are not encrypted and no authentication or integrity is checked the upper four are encrypted and contain Message Integrity Codes (MIC) where the MIC length can be 16, 32, 64, or 128 bits [27]. For encryption, Zigbee uses the AES algorithm in counter mode and for the authentication, the same algorithm is used but in block cipher chaining CBC mode. This combination is named AES-CCM and it is considered secure. While for the integrity and the replay protection Zigbee uses a message integrity code and a frame counter [28]. Two keys' types are used by Zigbee: network keys and link keys. The network key is known by all devices that are part of the network, it is used to secure message exchanged s at the network layer and it is exchanged via key-transport or transmitted by the trust center, for the link keys are used for end-to-end encryption at the application layer and all devices obtain this key either through Key-transport or pre-installed (by factory fabrication for example). Furthermore, some key negotiation protocols developed are used by some application profiles for key exchange. Eventually, the security between devices is guaranteed through a secure mechanism to initialize and install these keys [29]. The verification of the link key is done by using the Hashed Message Authentication Code (HMAC), where the hash function is a Matyas-Meyer-Oseas construction with AES-128 as block cipher [29]. The firmware updates of Zigbee devices is updated either wirelessly or Over the Air (OTA).

Z-Wave: The Z-Wave, which is a proprietary standard, is generally implemented in the HAN area for business and residence remote application control. The Z-wave protocol stack consists of the four lower layers of the OSI models: physical, data link, network, and transport.

The PHY physical layer is where data are transmitted. In Europe the Z-wave uses the 868 MHz band, while in the US it uses the 908 MHz ISM band. It is a low data rate protocol originally specified at 9.6 Kbps and then extended to reach the rate of 40 Kbps [39]. Z-wave also operates in the 2.4 GHz band with a data rate of up to 200 Kbps [25]. Usually, Z-Wave coverage can reach 30m for indoor and up to 100m for the outdoor applications; however, once a mesh network is in use, the coverage is unlimited. The network layer represents the routing abilities in which messages are routed between nodes and it contains a unique ID for the controller and a unique ID for each new device before joining the network. Usually, a Z-wave network consists of a controller and a slave. Controllers to define the network topology and the slave for sensor monitoring. The data link is the security layer where the encryption occurs and the MAC address is stored, whereas the MAC layer is used to avoid collision during frame transmission. The primary functions of the Transport layer are error detection, acknowledgment and retransmission. The Application layer appears on top of the protocol layers. Z-wave technology supports IP and is a low bandwidth control medium.

Z-wave Security Basics: In 2016 Z-wave alliance declared Security 2 (S2) update, which is required for all devices certified since April 2017. The security measures to provide confidentiality, authentication, data integrity, and replay attack are deployed by Z-wave at a distinct Security Layer within its security Command Classes. For robust security Z-wave has adopted a declaration of Security 2 (S2) which is classified into three subclasses: S2 Access Control, S2 Authenticated, and S2 Unauthenticated. AES-128 is the common encryption algorithm that is used by these tree classes. For the key exchanges, the Elliptic Curve Diffie Hellman (ECDH) which is considered secure enough, is adopted by S2 with a 256 bits public key. The 256 bits of key length is recommended by the German Federal Office for Information Security (BSI) [30]. to avoid low-security class forms impacting high-security classes S2 must define for each subclass its own network, this means that S2 Access Control and S2 Authenticated are separated from S2 Unauthenticated.AES-128 in CCM mode is used for encryption and authentication while AES-128-CMAC is used for integrity [31]. For all the legacy devices that cannot support S2, Security 0 (S0) for lightweight is there to provide them with security features. With S0 the network key like Zigbee is shared by every device in the network.

6LoWPAN is an acronym of IPv6 over the Low-Power Wireless Personal Area Network, it is a combination of IEEE 802.15.4 standard and Ipv6 to realize the IP enabled low power networks (for example for sensors and controllers). This combination between IPv6 and low power wireless networks is discussed by RFC4944 it specifies its format and features. This combination consists of adding an adaptive layer between the link layer and the network layer. This allows the IPv6 transmission over IEEE 802.15.4. Devices that are based on IEEE 802.15.4 transmit over a short-range with a small packet size of about 127 bytes and a data rate which varies between 250 Kbps for 2.45 GHz and 20 Kbps for 868 MHz. An analysis of home automation networks which adopt 6LoWPAN with IPv6 was discussed in [32]. They simulated home appliances using a web-based interface and they have discussed the utility and challenges of the combination of IPv6 and 6LoWPAN. Another case study discussing Ipv6 and 6LoPWAN's application. It emphasized the memory management of the device. Nowadays, and to integrate the IP functionality, suppliers are still trying to implement 6LoPWAN protocols, for example, the Zigbee Alliance has developed Zigbee IP which supports 6LoPWAN. The 6LoPWAN network topology is a mesh network that provides scalability and high availability. Since IP is supported by the majority of the most recent technologies, 6LoPWAN is considered a high-level interoperable technology.

6LoWPAN Security Basics: the 6LoWPAN vulnerability surface is a combination of WSN wireless sensor network vulnerabilities and IPv6 vulnerabilities. In order to secure the communication via 6LoWPAN the RFC4919 has defined the security requirements in terms of confidentiality, authentication, integrity freshness, and availability. Usage of cryptography ensure authentication, integrity, and confidentiality. As mentioned before since 6LoWPAN is the combination of IPv6 and WSN, it is normal to use the cryptographic mechanism used by both of them. AES is used by WSN to secure the Link layer however IPv6 is based on IPsec to secure end-to-end the network layer. With WSN it was judged that by using the public key technique it is heavy to use, but recently, new studies have shown that the combination of RSA and ECC works successfully [33][34]. For the key exchange, the IPsec key exchange that is based on network key exchange is not feasible and may not be adopted due to its heavy signaling messages and the 802.15.4 small packet size. The WSN adopts different techniques for key distribution like a pool of keys, pre-distribute key, and public-key cryptography.

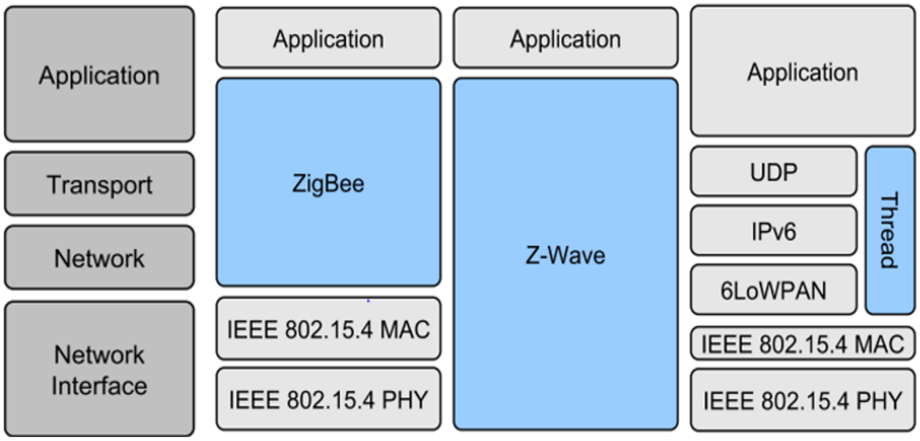


Figure 1-7: Protocols stack referring to the TCP/IP Model

LoRaWAN: Recently Semtech's LoRa/LoRaWAN has developed a new platform to address the indoor challenges faced of the above mentioned technologies. In addition to the IoT application extension to the home boundaries and into the garden, with the LoRa solution all IoT devices can be connected directly to the same platform where the range of old systems is too small. With LoRa there is no need for a mesh network and the implementation of repeaters due to the long-range coverage. In the following section, the LoRa will be further detailed and treated in terms of physical specifications and security features [35].

1. 6. 2 NAN Wireless Communication Network

The NAN area is made up of hundreds of smart meters creating a star, a tree, or a mesh network, which covers some houses or urban buildings. Different HANs can be connected to the same NAN and transmit for each home the energy consumption to the local data center through the NAN via the smart meter [36]. Measurement data is important and critical because it is used to manage the energy on demand generation and it is also used from the billing system. The NAN data rate is up to 2 Kbps, different technologies can be used for data transmissions like PLC which is a wired technology and WiFi, Wireless M-bus, LPWAN (NB-IoT, LoRaWAN, and Sigfox) and recently MIOTY which are all wireless technologies. Only wireless technologies will be presented in the following section

Wireless M-Bus: Compared to other existing protocols Wireless M-bus is relatively simple, so it has been widely deployed in Europe. The star network is adopted with sub GHz frequencies that offer long-range with a software stack of minimal size. the Wireless M-Bus standard operates in the 868-870 MHz, 433 MHz or 169 MHz Industrial Scientific and Medical (ISM) bands. Each European use their corresponding frequency bands, for example in France they used the 169 MHz frequency band combined with the 4GFSK modulation. In comparison with the TCP/IP model Wireless, Wireless M-Bus is slightly different. It consists of 3 main layers: the Physical, data link, the Network, and the Application one [37].

LPWAN: Generally used for long-range coverage where other technologies have failed and for low power consumption solutions. It offers a data rate of 250 bps to 50 Kbps per channel [38].

LoRa/LoRaWAN: LoRa wireless communication technology is patented form Semtech, and uses a chirped spread spectrum modulation for layer one or the physical layer for LoRaWAN. The chirped spread spectrum modulation decreases the interference impact on data transmission providing increased reliability. LoRa MAC developed by LoRa Alliance is the data link and network layer. Adaptive rate is one of the LoRa features, and can be changed accordingly with the chosen bandwidth. The transmission energy is defined by selecting the optimal spreading factor. The LoRa transceivers which must be integrated into the smart meter are inexpensive compared to other technologies. LoRaWAN uses the ISM frequency bands with a data rate that varies from 0.3 Kbps to 50 Kbps and transmits data within 5 km range in the urban area and 20 km in a rural area with a payload size of 243 bytes. In Europe, the adopted frequency band range is between 863MHz and 870MHz. LoRaWAN end devices operate in three different operating modes, namely A, B, and C, with each mode offering different uplink and downlink capabilities and energy requirements accordingly [39]. Class A nodes listen to incoming messages directly after the upload of some data and after that, they go back to sleep mode (batteries saving mode), for Class B nodes the gateway sends a beacon message to the end device that is used to synchronize time windows for listening and finally Class C devices are always in listening mode. LoRa networks are typically follow a star topology where the gateway is just a delay between the end node and the central server. The end node communicates with the gateway via LoRaWAN and the gateway communicates with the backend via the IP standard.

LoRaWAN Security Basics: The AES encryption is adopted by LoRaWAN at two security levels: network level and application level. The LoRaWAN provisioning process is based on the unique device ID and two keys. The first one is the network session key, which is used to secure the communication between the device and the shared network server, and the second one is the application session that is used to secure the data between the end node and the application server (application payload encryption). These Keys are exchanged via two ways: ABP which stands for Activation By Personalization where the keys are stored into the device and locked since the production deployment or via OTAA which stands for Over the Air Activation is based on a handshake process using a unique device key. With OTAA both keys were obtained from the same application key which has to be recognized by the network operator. However, the specification 1.1 raises a new AES-128 network key, this key has to be recognized by the network operator and it is used for obtaining the network key and managing the devices joining procedure while the application key is kept protected and in private. With LoRaWAN the end device ID protection is based on the device ID which is unchangeable for ABP devices and changeable for OTAA device. The CMAC algorithm with AES-128 encryption combined is used to generate a 4 bytes MIC that ensures data integrity. This MIC is derived from the network key and the MAC payload. To avoid any replay attack LoRAWAN relies on the counter field which is encrypted and integrated in every message. For data confidentiality AES-128 encryption is adopted in CTR mode, application payload encryption is based on the application session key. LoRaWAN end nodes supports two ways of communication and also support a multicast firmware upgrade Over The Air (OTA).

Sigfox: it's based on narrowband technology, can be deployed for long-range applications. It uses the BPSK (binary phase-shift keying) modulation in the uplink and Gaussian Frequency-Shift Keying (GFSK) in the downlink, it has a data rate up to 100 bps and transmits data up to 10 km in urban areas and up to 40 km in rural region [40]. Sigfox endpoints are inexpensive but the base station which controls and manages the network is more complicated than the corresponding element in LoRaWAN.

Sigfox protocol stack consists of: the physical layer PHY where Sigfox also uses ISM frequency band of 915 MHz in the US and 868 MHz in Europe. The MAC layer is responsible for the assembly and disassembly of data. The frame layer is used to generate the radio frame and finally the application layer which depends on the user's requirements. Sigfox is a cloud-based model in which the data is transmitted from the end device to the backend server through the gateway; it doesn't support the IP networking and like LoRaWAN it is suitable for applications that don't require large and frequent data transmission.

Sigfox Security Basics: generally based on symmetric cryptography, however not all security features are available by default. Sigfox provisioning process is based on three main identities the network key, the device ID, and the Porting Authorization Code (PAC). These credentials are transported in different ways either they are already stored in the device since the production or via Secure Element (SE) providers in addition to the possibility of using a Central Registration Authority (CRA). The main role of the network key is to encrypt the communication and it is only recognized by the CRA, by the SE and by the device maker. The device ID is a unique identifier for the end node and it is not encrypted or protected. The PAC can be used only for one time and it is used during the registration process to confirm the ownership of an end device by a specific group of devices. After any registration, the PAC is regenerated and transported to the group owner where it must be well protected and remained confidential to avoid any violation [41]. Sigfox defines two additional keys one is used for the authentication which is the same as the network but the network key is for the registration whereas authentication one is for the cryptography, the second one for the encryption it is functionality of encrypting the traffic exchanged between the end node and the core network, it is generated by combining the AES-128 with the network key. Sigfox data integrity is by cyclic redundancy check (CRC) field [42]. With Sigfox the data exchanged between the end node and the gateway are not encrypted by default, however, in 2017, Sigfox launched a new service to secure this exchange of data. This service is based on using AES-128 as an encryption key. For the end-to-end security, it should be done by the application developers. To avoid any replay attack Sigfox relies on the counter field that is encrypted and integrated into each message. It has field length of about 12 bits. In addition to the counter field, sigfox relies also on two timestamps; the first one is added to each message received by the gateway and the second one is added by the network server after a message is received [43].

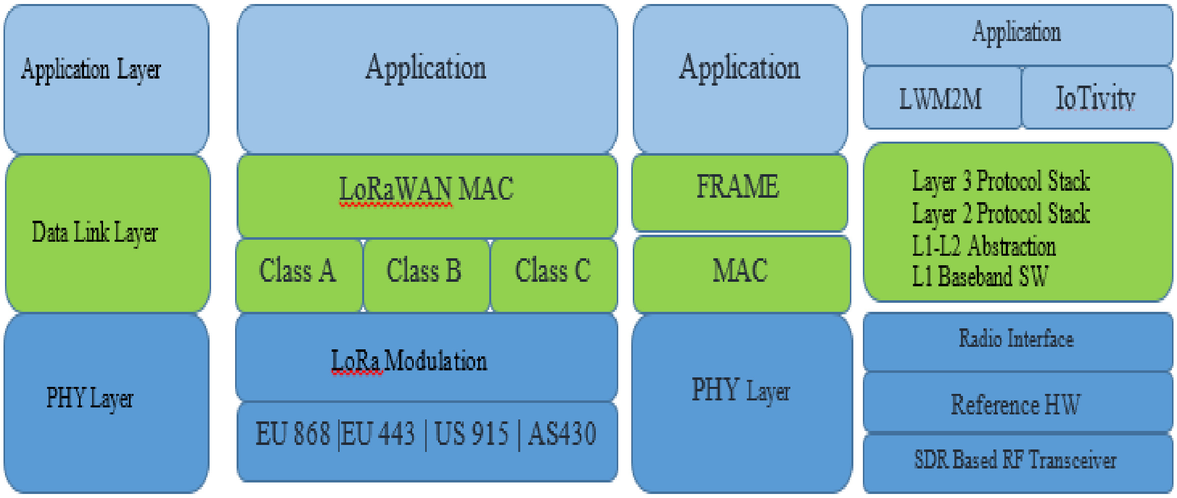


Figure 1-8: Wireless M-bus, LoRaWAN, Sigfox, and NB-IoT Protocols Stack.

Narrowband-Internet of Things (NB-IoT)

It is a standard developed by Third-Generation Partnership Project (3GPP), which uses the cellular telecommunication band to connect a wide range of nodes**.** It is used for M2M and IoT applications that require an extended range of transmission with a low cost and low power for long battery life. It coexists in the Long Term Evolution (LTE) or Global System for Mobile (GSM) under licensed frequency. The LTE functionality is deducted by NB-IoT at its minimum and its enhanced way of meeting the requirements of the IoT application. NB-IoT has a channel frequency bandwidth of 200 kHz, which corresponds to one resource block in GSM and LTE transmission.

NB-IoT can be operated in 3 different modes:

- In-band operation; utilizes, resource blocks (frequencies) within an LTE carrier that are otherwise used for mobile broadband resources.
- Guard band operation; It operates in the guard band immediately adjacent to the LTE carrier, without affecting the capacity of the LTE carrier. With this variety of choices, the operator can choose the most suitable operation mode to satisfy its network performance requirement while offering the services to IoT applications
- Standalone operation mode; it uses the GSM low band (700MHz, 800MHz, and 900MHz).

However, the 3rd Generation Partnership Project (3GPP) recommends the use of the In-band operation mode. Since the NB-IoT protocol is based on LTE it uses the LTE protocol stack (the physical and the upper layers). QPSK modulation, Frequency Division Multiple Access (FDMA) is used by NB-IoT for the uplink, and the Orthogonal FDMA (OFDMA) is used for the downlink. The data rate can reach up to 200 Kbps in downlink and up to 20 Kbps in the uplink, with a payload size of 1600 bytes for each transmitted or received packet and it sends data for 1 km in an urban area and up to10 km in a rural area. NB-IoT can support up to 50K devices per cell and this number can be expanded using multiple carriers. In 3GPP release 15, new improvements were introduced, such as multicast services that are used by NB-IoT for end-nodes firmware update[44].

NB-IoT core network consists of the evolved packet system (EPS), and two enhancements for the cellular internet of things (CIoT): The User Plane CIoT EPS, and the Control Plane CIoT EPS. Both planes select the optimal path in both directions (uplink and downlink) for control and user packets. The process by which NB-IoT users access a cell is similar to the LTE procedure. The evolved UMTS Terrestrial Radio Access Network (E-UTRAN) which consists of eNBs, controls the RF communication between the User Equipment (UE) and the Mobile Management Entity (MME) at the control plane and the transmitted data between UE and Packet Data Network Gateway (PGW) through Serving Gateway (SGW) at the user plane. Non-IP data will be sent to the application server via the Service Capability Exposure Function (SCEF) through the control plane. However, at the user level, both IP and non-IP transmit the data over radio carriers to the application server through the SGW and PGW[45].

In the uplink and download link, both Control Plane and User Plane select the optimal path for control and user packets. Access to the NB-IoT network is similar to access to the LTE network. As a conclusion, the E-UTRAN architecture and the backbone network can be used for NB-IoT.

NB-IoT Security Basics

The security mechanisms adopted by NB-IoT are similar to the LTE system that was developed from. Entity provisioning process: Authentication in NB-IoT is based on the EU first affirming a unique identity so that the network can then verify that the EU credentials match that identity. There is a hypothesis, thus, that the identifier is unique and always assigned to a specific

UE, otherwise, any authentication of that identity is denied. To ensure the confidentiality and integrity of data NB-IoT uses four algorithms: the NULL which means no security mechanism used, the SNOW3G based 128-bit stream cipher, the AES based 128-bit block cipher in CTR mode, and the ZUC (Zu Chongzhi) based128-bitstream cipher.

For data, confidentiality is controlled in NB-IoT by Non-Access Stratum (NAS) commands. As well, the previous three cipher algorithm built on symmetric cryptography is adopted. Against the replay attack, NB-IoT uses the Key hierarchy to protect and encode the NAS signaling messages exchanged between the EU and the MME. For firmware updates, the OTA is supported by NB-IoT only in IP mode. The NB-IoT core network is IP based, the network traffic can be monitored using a firewall. The network can be monitored in real-time by mobile network inner mechanisms[42].

MIOTY: Developed by Fraunhofer-IIS, it is a new Telegram-Splitting Ultra-Narrowband (TS-UNB) technology. It provides a reliable and energy-efficient solution for every application system. It is possible to have a variety of transmissions simultaneously with only one unit receiver without interference. Due to low self-interference generated, the system can support up to one million simultaneous transmitters [46]. The transmission range is up to 15 Km in a flat area and 5 Km in an urban area. MIOTY channel encoding scheme increases its range by a factor of 10 compared to the 868MHz wireless standard [47]. MIOTY is better than the current cellular and non-cellular existing LPWAN technologies because it's more robust and resistant to interference from other systems. MIOTY secures the network with an integrated AES-128 device.

1. 6. 3 AMI Communication Technologies Comparison

SM, which is a main component of the AMI network, wireless communications technologies are divided into two categories the short and long-range wireless communications technologies. To expand the coverage, limit due to their physical short-range (less than 100m), wireless technologies (e.g. Zigbee and Z-wave) use mesh network topology. However, the main disadvantage is their high deployment cost to connect the large number of nodes that are geographically scattered throughout a large area. Furthermore, since the data is transmitted via multi hops to the gateway, a large number of nodes are more loaded and congested than others which will have an impact on the life of their batteries (i.e. excessive use of energy) and so the lifetime of the network will be affected. This restriction is resolved by LPWAN technologies (Sigfox, LoRaWAN, and NB-IoT), which are based on star network topology, where end nodes are directly connected to the gateway. Unlike the mesh network, before sending data, the end node doesn't listen to the radio channel, which guarantees energy savings. And since gateways are always online, they ensure instant access to connected nodes. However, compared to LPWAN short-range technologies, the data rate is higher as it is between 250 bps and 200Kbps for LPWAN and 250Kps for Zigbee. As well, not all LPWAN technologies are equal in terms of coverage, cost, data rate, latency, scalability, standardization, and energy consumption. LPWAN technologies operate on both the licensed (e.g. NB-IoT) and unlicensed (e.g. MIOTY, LoRa, Sigfox, etc.) spectrum. NB-IoT, which has faster response time than sigfox, and LoRa, guarantee a better quality of service (QoS) since it is based on the time slotted of LTE synchronous protocols, while LoRa and Sigfox do not support any QoS. NB-IoT operates with a data rate of 200Kbps where the maximum data rate is around 50Kbps and 100bps, for LoRa and Sigfox respectively that are much lower than NB-IoT. In an urban area, Sigfox can transmit data over 10 km where LoRa and NB-IoT transmit data at 5 km and 1 km respectively. LoRaWAN and Sigfox consume less energy than NB-IoT by reducing their energy consumption in sleep mode, which will save the battery life of the device. Hence, for an application like Smart City, Smart Building where low data rate, low-cost solution, long battery life, and no QoS are required LoRa/ Sigfox are the best suitable technologies, however in applications, where high data rate, low latency, QoS, scalability, and standardization to ensure a secure, reliable, and interoperable network, are the main concerns, NB-IoT deployment is preferred.

1. 7 AMI Cyber Security

The Smart Meter is the first point that is responsible for gathering the energy consumption data for the power grid. As mentioned previously the smart meter consists of two network communication interfaces and a serial port for access and maintenance. Since internal serial links are not protected any physical access to the smart meter can expose the whole system to some security vulnerabilities. Embedded Microcontroller security leaks, radio interfaces, and firmware updates expose consumer privacy and introduce cyber-physical vulnerabilities. The Advanced Metering Infrastructure (AMI) is currently being implemented quickly across the power grid and allows technology to be introduced to the smart grid. With its rapid, huge, and extensive deployment AMI security has become an area of focus with the following main directions:

- Data collection
  - Data availability which means that the network is always in operation.
  - Data confidentiality is necessary to maintain data privacy and to avoid data exposure to unauthorized parties, it can be guaranteed by data encryption techniques. Data freshness is required to make sure that the data is new and recent, it is guaranteed by the adoption of counter and timestamp techniques.
- Network management and provisioning
  - Authentication: The authentication is used to verify if an entity has the right and privilege to access, participate and join any network and finally non-repudiation which is a way to be sure that the sender has no way to deny of having sent a message and the same for the receiver, this security requirement is essential to avoid replay and data injection attacks and it is guaranteed by the use of public-key encryption with a digital signature.
  - Authorization: This guarantees that only certified devices are allowed to access, use, or control the system and violate what is authorized.
  - Non-repudiation: This indicates that only authorized devices can receive data and do not refuse to receive it later. Some devices may not indicate when data is received if it is not. Therefore, no false alarm of exchanged data is taken into account, i.e. an end of the system may not deny any measure or action taken by the AMI.
  - Initial provisioning and secure firmware update. Whether performed On The Air (OTA) or with a physical connection.
  - Accountability is used to verify every action taken by the system. it is similar to the Non-repudiation
- Reporting

- Monitoring and Analysis give the AMI system the ability to examine itself and try self-healing. AMI systems must be able to provide automated control in cases of any internal or external problem and transmitting these records for further examination, processing, and analysis.

- Furthermore, contemporary AMIs are designed to support Smart Grid processes built on top of it (e.g. DR scenarios with active involvement of consumers, aggregators, ESCOs, etc., Demand Side Management scenarios will be supported by providing real-time analytics and modeling of the micro grid operation, etc.), in near real-time, including energy demand, storage and supply (even including self-production when applicable), which raises the bar even higher in terms of speed, and security for optimizing energy production of the micro grid.

These mentioned requirements are mandatory and essential to guarantee data security. Therefore, the definition of the attack surface is mandatory to secure the smart grid and the AMI. The following will define the surface attack of AMI and especially wireless technology[48].

Communication Network and Technologies Security Vulnerabilities

Usually, the communication network is used to connect the various components of the AMI (for example to connect the SM to the Data concentrator). In addition, the AMI information network connects the HAN (the consumer side by using Zigbee, Z-wave, or other wireless technologies) to the NAN. These communication networks are geographically distributed across the smart grid. These networks consist of hundreds of thousands of devices including smart meters and data collectors that are forecasted to have a long life and are widely implemented. By deploying that large number of long life devices, and taking into consideration the cost impact, means that hardware replacement is not that easy and any future firmware upgrade will be difficult. These constraints will increase the vulnerability of the AMI system to intrusion if a single SM is compromised over time.

By adding the extensive use of wireless protocols by AMI, the risks of cyber-attacks increase and so too the system vulnerability. Although these protocols have been used for a long time ago and that are widely adopted, they are still the main target for attacking the Smart Grid infrastructure. Usually, they use AES for data encryption. Some of these protocols have weak encryption and vulnerable key exchange processes that can threaten the data integrity and compromise the system. A discussion of the security vulnerabilities of the mentioned wireless communication technology will be presented in the following section.

Zigbee Security Vulnerabilities:

Physical attacks: These attacks target critical and sensitive information stored in devices. This information serves to initiate various attacks against the Zigbee network.

- Insecure Key Storage: Zigbee protocol's security is based on the assumption that its keys are stored securely. Typically, the network key is preconfigured within the coordinator, but for the link key, it is preconfigured for routers and end devices. Unsecured storage of any of the networks, links, and master keys would make it easier to extract the key, compromising the overall network.
- RF interference: while Zigbee adopts some reliable techniques to protect the network from interference, but they are slow to be executed and not completed, which allows the attacker to take control of the frequency channel as the network is running.
- Network Spoofing: Zigbee allows the link key to be reused for rejoining the network. Therefore, an attacker can copy an end device's credentials and join the network with a different device. As a result, the trust center passes the network key encrypted with the previously used link key to the cloned device, which will allow the attacker to get access to the entire network.

Cyber Attacks:

- Insecure Key Transportation: any node that joins the Zigbee network gets its network key over the air. In case the key is sent in plaintext an attacker can get the key through eavesdropping and will compromise the network as this key is shared between all network devices.
- Unencrypted Security Headers: Usually the auxiliary frames are used to ensure replay protection. However, when an attacker generates a false security header but does not know the key behind creating the MIC, even if attacks on data integrity fail, the receiver will

spend a considerable amount of energy to process these false messages that will lead to battery exhaustion. This what we call a ghost-in-wireless attack.

Other Attacks:

- Replay attack: as well as Zigbee's instructions and specifications have adopted mechanisms to stop the replay attack, but 802.15.4 has restricted replay security techniques, which cannot be improved even with an encrypted message. Therefore, an attacker can replay an earlier message without changing the content (since Zigbee restricts the modification of the packet) until key rotation. Different attacks come with the replay attack, like DDOS where a suspicious user in the network receives packets and replays these packets to disrupt and interfere with the total functionality of the network.
- Man in the middle attack: for packet acknowledgment, Zigbee instructions do not ensure integrity and confidentiality security. By consequence, a non-validated attacker can spoof the acknowledgment packets and make the sender think that the packet is well received by the real recipient. In other words, if the sender doesn't receive an ACK packet he will retransmit the same packet, if the network is compromised and the ACK is unauthenticated, the attacker can intervene and send a false ACK to the sender. Then the sender will transmit all the remaining packets to the attacker.
- Information theft: like any other wireless protocol Zigbee is at risk of statistical attacks that exploit the weaknesses of a targeted algorithm. These types of attacks compromise the end-user's privacy, allowing an attacker to gather and collect critical information. [49]

Z-wave Security Vulnerabilities:

Pairing vulnerabilities: To protect the traffic Z-wave uses a shared network key. This key is transmitted between the controller and the end device during the pairing process. These keys are used to secure the communications and prevent hackers from compromising joined devices. The previous Z-wave pairing S0 mechanism is too weak and vulnerable, where the network key has been shared between nodes by using a key of zeroes which is easy to be sniffed by a hacker within the RF coverage and once the network key is obtained the attacker can have access to control the Z-wave network. Hence Z-Wave has improved and fixed this pairing process by Z-Wave S2. But unfortunately, recent studies have shown that even it's not easy to hack Z-Wave S2 but it can be downgraded back to S0, canceling all security improvements. The downgrade attack requires physical proximity to the device while the pairing process [50].

6LoPWAN Security Vulnerabilities

6LoPWAN stands for IPv6 over low-power Wireless Personal Area Networks, hence its security vulnerabilities come from both networks. Also, there some vulnerabilities that point to the adaptation layer.

Physical attacks:

- Jamming: this attack tends to perturb the operation of the network and this is achieved by transmitting high energy signals to continuously occupy the channel which will cause transmitter failure. To stop such types of attacks spread spectrum techniques are used.
- Radio Interference: where the attacker generates a big amount of interferences discontinuously or constantly to deteriorate the legal signal result in the receiver failure.
- Tampering: when an attacker gets access to the end device, he can extract some critical information such as cryptographic keys. These types of attacks can be avoided by node tamper-proofing or by self-destruction when anyone physically accesses the device, the nodes erase their memory which prevents any information leakage.

Outside/ Inside Attack when an attacker is out of the network and get illegitimate access to listen or initiate DoS attack by jamming or power depletion. Usually, to protect against such types of attacks, to avoid strangers from accessing the network, systems deploy cryptography mechanisms. But these techniques are not effective in protecting against compromised internal devices. There are many ways to compromise an internal device. for example, any physical attack can guarantee the attacker the ability to retrieve the cryptography key or to change the firmware of the device. Usually, this type of attack points to spoil a network operation. These attacks are too dangerous as they can simply be launched and harm network operation, for example, a Sybil attack which is a link-layer attack. First type of link layer Sybil attack type concerns the data aggregation where a compromised node acts differently and then this may cause many negative reinforcements to make the aggregate message a false one. Second type is Voting. Many MAC protocols may go for voting for finding the better link for transmission from a pool of available links. Here the Sybil Attack could be used to stuff the ballot box. An attacker may be able to determine the outcome of any voting and off course it depends on the number of identities the attacker owns. In addition to some attacks that are related to the IPV6 network, where the neighbor discovery and address auto configuration mechanisms are adopted. These mechanisms are exposed to some threats, as an attacker can get into these processes and spoof the neighbor solicitation/ advertisement [51].

Adaptation layer threats: This layer functionality is implemented on the edge router between the two networks IPV6 and WSN. Usually, this edge router is very well secured and protected but the packet fragmentation and reassembly are still subject to some threats. Some of these threats are tiny fragmentation, frag router attack, such attacks will lead to significant node damage (like buffer overflow due to packet re-sequence).

LoRaWAN Security Vulnerabilities

Physical attacks: network devices may be used by attackers to launch the attacks listed below.

- Taking out Security Variable: LoRaWAN instructions insist on securing of the relevant key material against reuse. But if an attacker gets direct physical access to the device, the possibility to changing the firmware or thieving / reusing the key material becomes easy. Therefore, devices should be secured against any firmware alteration that can guide reuse or thieve of the key material.
- In LoRaWAN session keys derived from the root keys that are usually are produced during manufacturing. Hence, breaking of a root key will only compromise the data stored in this device. This information can be accessed only by destroying or stealing an end device.
- Insecure Key storage: if Keys are stored in plain text files within the end device and the security storage requirements are not satisfied then plaintext Key Capture attack is a serious danger that will compromise the confidentiality, integrity, and availability of the network.
- RF Jamming Attack: the use of low-cost hardware makes the RF jamming possible. RF jamming may cause DoS (Denial-of-Service) that is easily detected. However, selective RF jamming attacks are more difficult to catch and therefore damaging to wireless protocols as it is not easy to avoid.

Cyber Attacks:

Eavesdropping attack: it occurs when the attacker relays on the weaknesses which reside at the level gateway to receive packets and conclude some information about the transmitted data and the adopted key material. However, without getting the key material, an attacker cannot decode the packet contents.

Other Attacks:

Man-In-The-Middle (MITM) attack: there are two attacks under MIM the first one is a bit-flipping attack in which the attacker modifies the message content while the message is being transmitted between the network server and the application server. The second attack is frame payload attack this attack is due to the handover-roaming as the unprotected FRMPayload messages are first transported from the serving-NS to the homing-NS, and from there to the AS.

Replay attack: to access the network an end device must retrieve the key materials that should be well protected. A way for an attacker to have access to these credentials, either by taking control of a device or by changing the firmware to make it possible to reuse key materials. End devices are sources of information that they cannot modify data at the network server. Hence, any compromised device cannot leak data from the network, it can only inject fake information to the application server. A compromised device can be used to launch a replay attack. All packets that are transmitted by the remaining devices can be captured and replayed subsequently. In general, this attack detected by the use of the nonce values, but this will lead to available resources occupation and reduce the availability of the gateway to serve the non-malicious devices.

Self-Replay Attack: The OTAA is developed to improve LoRaWAN security. However, by itself, it becomes a subject of attacks. By using the selective RF Jamming mentioned above, an attacker can compromise LoRaWAN joining process. However, a professional attacker is able to selectively jam the signals that are generated during the OTAA process. In this case, the Join-request with DevNonce sent by an authorized end device is detected successfully. Applying the selective-jamming methods Join-accept message sent by the network server to the end device is jammed. The end device waits to receive the Join-accept, after a period of time if it doesn't receive this message, it will resend again the same Join-request with DevNonce to join the network, the sever on its side will send again the Join-accept since everything is legitimate and the joining process is not yet completed. This exchange of data will continue until the quota of messages of the end device is exhausted since with OTAA the exchange of messages is restricted and under quota. To succeed an attacker would have to receive packets sent by the network server before reaching the end device [51].

Sigfox Security Vulnerabilities

Replay attack: the 12-bit Sequence Number (SN) is used to protect Sigfox from a replay attack. It is secured by Message Authentication Code (MAC) and sent to every uplink frame. The server will discard any packet that has a SN lower than the latest packet received. MAC calculation is not public, but some of its inputs are AES in CMAC mode combined with the Network Authentication Key (NAK) and the SN. For downlink packets, there are no public details about the size of the SN, so there is not enough details about the security of downlink messages as compared to uplink messages. The 12-bit SN of the uplink packet allows 4096 unique messages, then the SN is reset back to 0. Since Sigfox NAK key (which is used for MAC calculation) is static through the node lifetime, replay attacks become a serious possible threat to Sigfox. Sigfox SN number resets approximately every 30 days based on the maximum number of uplinks packets that can be sent daily by Sigfox. In practice, the Sigfox end device can still send packets even beyond the limit, and these packets can still be received and accepted by the server, which leads to an early SN reset. After resetting the SN, the hacker can replay one of the previous frames indefinitely, as the NAK key used for the MAC calculation is static and unchangeable, which means that the MAC will ever be valid during the lifetime of the compromised node [52].

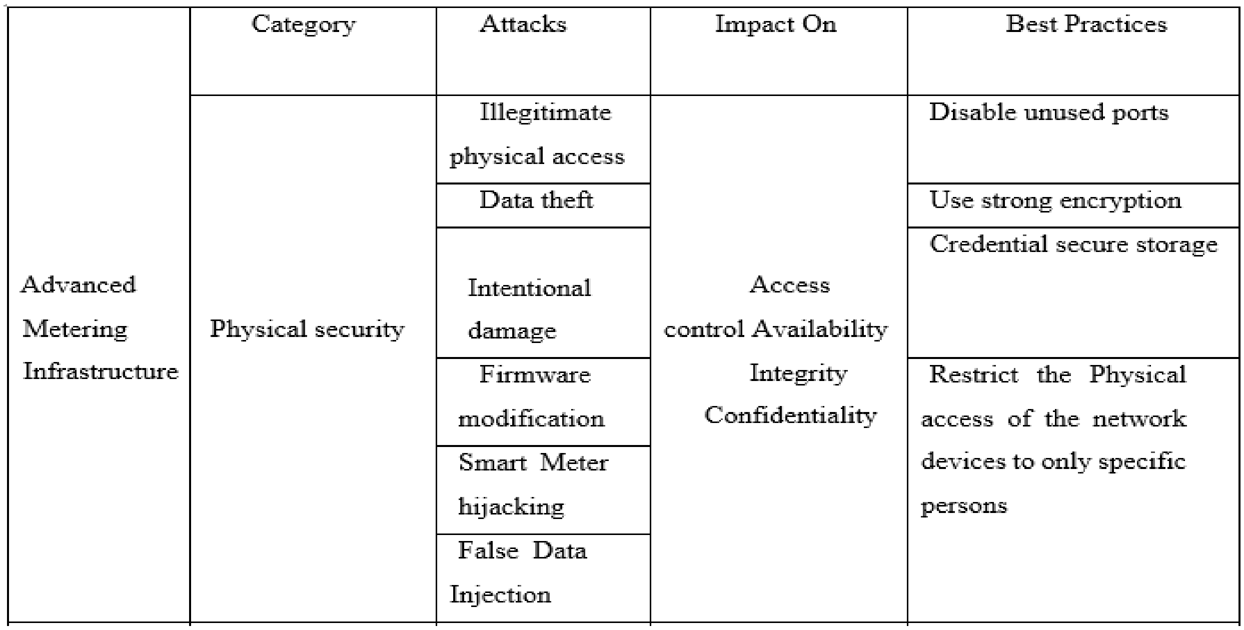
NB-IoT Vulnerabilities

Denial-of-Service (DoS) attacks: Invisible threats in NB-IoT nodes come from their scale. There is a high potential for launching denial-of-service (DoS) attacks by exploiting a group of devices to send unexpected communications to specific victims. In addition to a service disruption on the victims' services side, such type of attacks has also an impact on the service provider’s network which cause a service deterioration due to a signaling load prohibiting the remaining uninfected devices from sending, receiving data, and responding to their control requests [53].

1. 8 AMI Security Best Practices

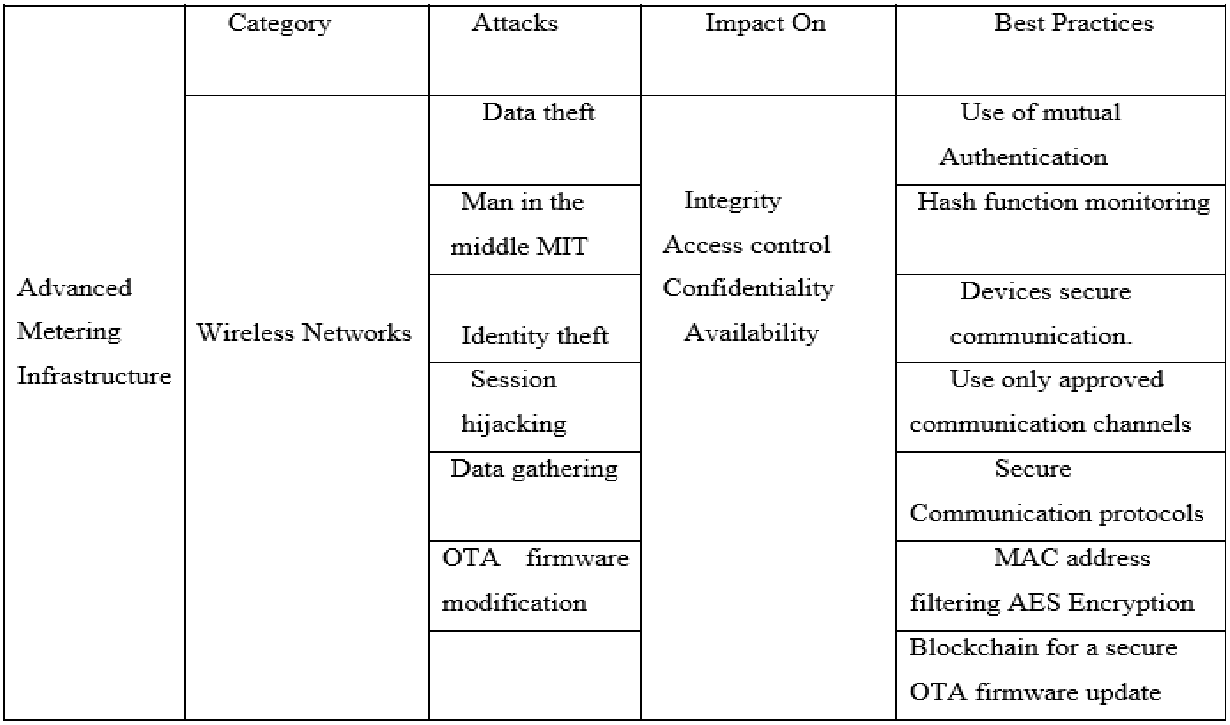
In order to protect the Smart Grid against all potential cyber-security threats, defense strategies and some good practices need to be adopted and integrated at the AMI level including wireless communication protocols and the architecture in use. In addition, the security of all participating components, which addresses the security of each component including the SM, must be performed and tested. It covers device conformity, functionality, and interoperability testing.

The most relevant attacks against AMI, their impact on the system, and the recommended published best practices are summarized. There are several best practices released for all aspects of Smart Meter, AMI, and communication networks/ technologies that can be concluded from the previous sections where we have discussed their security gaps and vulnerabilities that can lead to a compromised system. The below tables1(a)(b)(c) mainly focus on Smart Meter devices, wireless communication technologies, and communication networks in general [54]. Based on different categories within the AMI, it represents different attacks that we could face and the practices to avoid those types of attacks



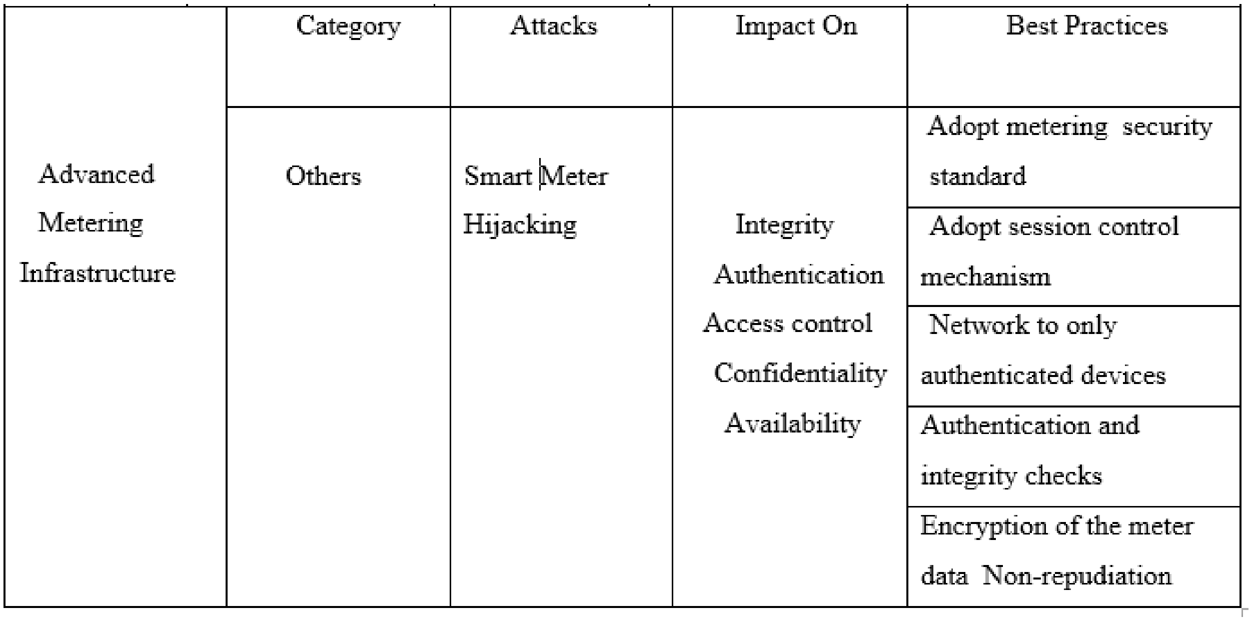
	Category	Attacks	Impact On	Best Practices
Advanced Metering Infrastructure	Physical security	Illegitimate physical access	Access control Availability Integrity Confidentiality	Disable unused ports
		Data theft		Use strong encryption
		Intentional damage		Credential secure storage
		Firmware modification		Restrict the Physical access of the network devices to only specific persons
		Smart Meter hijacking		
		False Data Injection		

Table 1-1 (a) Physical Attacks



	Category	Attacks	Impact On	Best Practices
Advanced Metering Infrastructure	Wireless Networks	Data theft	Integrity Access control Confidentiality Availability	Use of mutual Authentication
		Man in the middle MIT		Hash function monitoring
		Identity theft		Devices secure communication.
		Session hijacking		Use only approved communication channels
		Data gathering		Secure Communication protocols
		OTA firmware modification		MAC address filtering AES Encryption
				Blockchain for a secure OTA firmware update

Table 1-2 (b) Wireless Attacks



	Category	Attacks	Impact On	Best Practices
Advanced Metering Infrastructure	Others	Smart Meter Hijacking	Integrity Authentication Access control Confidentiality Availability	Adopt metering security standard
				Adopt session control mechanism
				Network to only authenticated devices
				Authentication and integrity checks
				Encryption of the meter data Non-repudiation

Table 1-3 (c) Other Attacks

1. 9 Security Recommendations Summary

Over the last decade, information systems have undergone a major transformation from proprietary, isolated systems to open architectures highly interconnected with other corporate networks and the Internet. As well, Critical Infrastructures (CIs) is becoming huge infrastructures with multiple access points. However, CIs have expanded, and communication protocols have been developed with no security in mind. Physical attacks of IoT nodes, especially in the case of interconnected nodes, compromise not only the node but also the network security and are more difficult to identify. This exposes CIs to a various physical or cyber threat.

As a result, the evolution of power grid systems has led to a significant improvement, which has brought benefits to the utilities, consumers, and the environment. The integration of Smart Meters, the introduction of wireless protocols, and the adoption of a bidirectional communication have raised the need for secure communication to protect the data transmission. The AMI which is part of the smart metering network system is responsible for the transportation of metering data, including billing data and other information. The smart meter network is composed of a large number of smart meters that interconnected through different wireless protocols to provide the metering data to the control center.

All the SG structure is largely based on the communication networks and the secure delivery and management of smart meters data. This dependence and the software-oriented management of the underlying network make the SG vulnerable to a wide range of threats. These potential threats or attacks could cause many problems in the SG ranging from physical damage to blackouts. Also, attackers could have access to electricity companies and customer's information. In the United States, CIA’s reports have already revealed that hackers have turned off the power in several cities after breaking into electrical utilities and demanding extortion payments before disrupting the power [55].

The U.S. National Institute of Standards and Technology (NIST) has already produced a report that presents a cyber-security strategy and architecture. The document identifies a set of risks for SG such as:

(i) Vulnerabilities and exposure to attacks or accidental errors.

(ii) New vulnerabilities generated by the interconnections across networks.

(iii) Vulnerabilities and weaknesses caused by communications network disruptions of the introduction of malicious software.

(iv) Increased number of entry points and paths available for potential adversaries to exploit.

(v) Threats to the confidentiality and integrity of data caused by interconnected systems that may increase the amount of private information exposed.

(vi) Vulnerabilities introduced by the use of new technologies or potential to compromise the data integrity e.g., customer privacy breaches as a result of increased data collection.

The main problem is that, while the SG exposes the electrical infrastructure to a software guided framework managed by computer-based control systems – at the same time, these systems are increasingly connected to open networks, such as the Internet, exposing them to cyber risks.

Due SGs heterogeneous communication architecture, a challenge is to develop sophisticated and robust security mechanisms that can be easily deployed to protect the management of data and the communications between different layers of the SG infrastructure.

We not only need assistance to define models and mechanisms for identifying threats, but also to define plans for the (pro-) active response to the presence of threats and the relevant recovery methodologies to avoid any negative consequences on the SG performance. Threats will be categorized according to specific security goals set for:

(i) Electricity companies or grid operators,

(ii) Customers and,

(iii) Home/business environments.

Considering three overall tiers (i.e., layers): **(i)** the first tier is related to security management in the smart meters, **(ii)** the second tier is related to the security management in the concentrators' level and, **(iii)** the third tier is related to the security management at the operator's level. Concentrators aim to manage the data coming for a number of smart meters, creating a set of 'islands' (i.e., a subset of interconnecting smart meters based on spatio-temporal characteristics). Different technologies will be adopted at each tier focusing on different threat categories. Provides a holistic framework to improve SG infrastructure resilience. It is capable of managing both physical (electrical) and cyber threats that are rapidly detected so that remedial actions are affected. Offers a framework that is capable of responding to a dynamic environment like the SG and provides concrete solutions to deal with any security leakage in the infrastructure by maximizing its performance.

1. 10 Conclusion

AMI which is a crucial element of the SG faces various security threats. Countermeasures for SG attacks in terms of physical or cyber-attacks will be focused on a sensor/actuator infrastructure (IoT devices), secure networking functionalities, and automatic – if possible – the neutralization of any attack against critical infrastructure element. This chapter presents a detailed approach of the AMI system with respect to the different components and sources of threats. It examines the communication requirements for the AMI and discusses the communication architecture that is based on the HAN, NAN, and the WAN. Various communication technologies for AMI applications are discussed in terms of communication coverage, basic security measures, and privacy. It was then necessary to conduct a study on security vulnerabilities, challenges, and attacks. The specifications of each protocol were very well defined in terms of coverage, frequency band used, data rate, and protocol stack. The first security objectives to be met were to identify the security mechanisms adopted by each protocol in terms of the encryption algorithm, key exchange process, and authentication process, then, the potential attacks and security vulnerabilities of each protocol were described in terms of three categories the physical attacks, the cyber-attacks, and other remaining types of attacks. The second security objectives to be achieved have been identified by the list of potential attacks targeting the AMI requirements, in terms of availability, integrity, control, and authentication, which directly affect the functionality of the AMI system. For the next chapter, it will be based on the AMI architecture and our designed and developed prototype will communicate with other components using LoRaWAN technology and will respect the predefined security basics.

Chapter 2 : Internet of Energy: State of the Art, European Scenarios.

2. 1 Introduction

The energy industry is currently facing major challenges. The growing energy demand has led to a lack of fossil fuels which has caused a sharp increase in energy prices, on the other hand the ability of the atmosphere to absorb CO2 emissions is also exhausted. That has pushed efforts towards climate protection and the efficient use of energy.

Secondly, the increase in the use of Renewable Energy Resources (RES), which has led to efforts to integrate these resources into the grid, both in the increased decentralized stations and the current central stations. Therefore, it is necessary to have a higher degree of flexibility in terms of maintaining the voltage and efficient control of the load flow that is used in the existing system.

Moreover, the regulatory change of the environment has imposed new and modern requirements regarding the interconnection of information between energy frameworks. Due to decentralized power generation, transmission and distribution, various facilitators along the value chain transmit and collaborate through common interfaces. In addition, new rules on standardization, metering, and transparency of use generate huge amounts of information to be processed.

Finally, the latest technological developments can no longer be ignored. New demand response solutions, smart meters and energy-saving innovations are attracting energy markets and are being progressively used by both energy providers and energy consumers. All these variables require a transformation to an intelligent and efficient supply system, which is interconnected through information and communication systems (ICT) - the Internet of Energy (IoE).

IoE is a subject related to the Internet of Things (IoT), communication system, smart grid and low carbon technologies. It is significant for the techniques of Industry 4.0 as well as for the Energy Strategy 2050. Thus, the AIOTI, the European Alliance of IoT Innovation encouraged by the European Commission, has a particular working group on smart energy and a few others on IoE topics to help disseminate this new technology in markets and businesses. However, despite the fact that the IoT innovations are growing rapidly, progress on IoE is slower than anticipated. Lack of awareness of IoE developments and a missing image of the state of the art of IoE in general are among the reasons that hinder IoE dispersion in related areas.

This chapter provides an overview of current and future IoE advancements, use cases, applications and related action plans in Europe will be provided. Particular attention will be given to the introduction of the current state of IoE in Europe countries like Germany and Greece. The German system will be presented and discussed in detail since it was used as a reference architecture of our developed energy metering gateway.

2. 2 Internet of Energy

2. 2. 1 What is Internet of Energy?

The term 'Internet of Energy', or 'Energy Internet' was first introduced by the American macro-economic forecaster Jeremy Rifkin in his book 'Third Industrial Revolution' in 2011 [1]. He expected that many individuals would generate their own sustainable energy at their premises and factories and offer green energy in an 'Energy Internet' such as how the data was produced and shared by the web. Accordingly, IoE represents the web style solution for the power system that is based on a bidirectional data communication and power flow [2] and could be considered the expansion of a Smart Grid.

It is important to distinguish between IoE and Smart Grid as both terms can be used synonymously. While the Smart Grid focuses mainly on a smart energy distribution infrastructure that depends on a solid high speed communication network for verification and control, IoE covers the full range of energy demands, including electricity and gas [3].

The analysts of the European project ARTEMIS1 dedicated to electric versatility also noticed the bidirectional nature of the IoE and characterized it as "a network infrastructure dependent on norm and interoperable gateways, conventions and protocols that permit a continuous equilibrium between the neighbourhood and global production and storage ability with the energy demand, also permitting high level of customer awareness and participation" [4]. In addition, Vermesan et al. presented the ability of the new Internet-based framework to fully implement distributed energy resources to achieve a robust, adaptable, effective and smart energy supply system.

From a business point of view, the main characteristics of IoE are openness, operation, uniformity, sharing and personalization within the entire operation of energy production and use.

In this context, IoE becomes an innovative technology tool, a support platform and indeed a generalized asset, which can change the lifestyle of people and the activity of businesses. Hence, the improvement and development of an energy framework is essentially developing a management concept and service models [5].

For researchers in the technology market, IoE is a disruptive data and communication technology (Internet of things and cloud computing) that will have an impact on the energy system moving from a traditional system with a centralized energy production and storage and from one-way power flow direction to decentralized energy system, starting from the consumers to the prosumers who are now able to generate and manage their own energy.

IoE is therefore the smart ICT-based interconnection among all the devices of the energy system, such as PV systems, transmission and distribution system operators, consumer components, prosumers, and clients with the goal to guarantee sustainable energy generation and smart utilization. IoE has a significant effect on the energy sector at different levels, starting with energy production to consumption in residential premises and at commercial buildings. Figure 2-1 shows the world of the IoE in growth and the impact generated as follows:

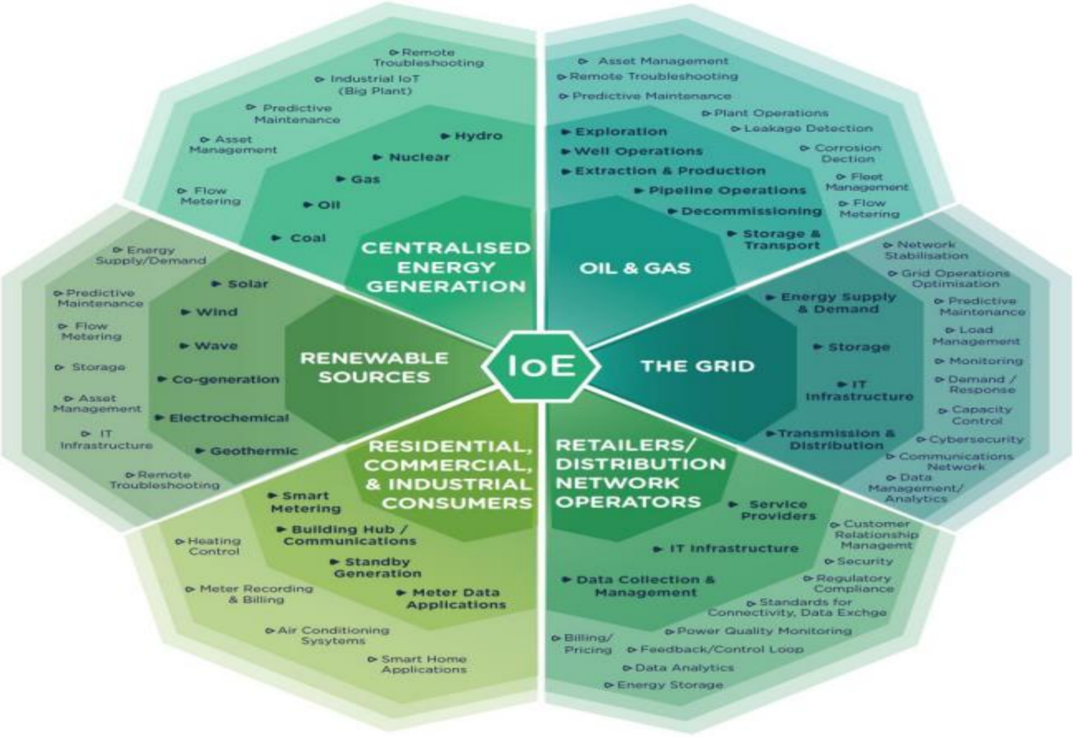


Figure 2-1: The World of IoE [6]

This is to give a short view of the new phenomenon known as IoE. For a deeper understanding of the IoE world, it is crucial to have a close look to the IoE architecture**.**

2. 2. 2 Internet of Energy Architecture

IoE architecture refers to communication infrastructure and addresses both the energy and data exchange between different resources and loads, such as sustainable energy sources distributed energy storage, residential and modern buyers [7]. These communication measures are monitored and verified through the Internet. The overall guideline is that energy and data streams are guided from the sources to the destination like data stream in the Internet. The Internet of Things (IoT) is seen as the technology that can be used to facilitate the two-way communication. Figure 2-2 shows the interconnection between the different components and shows the complete IoE communication architecture [8].

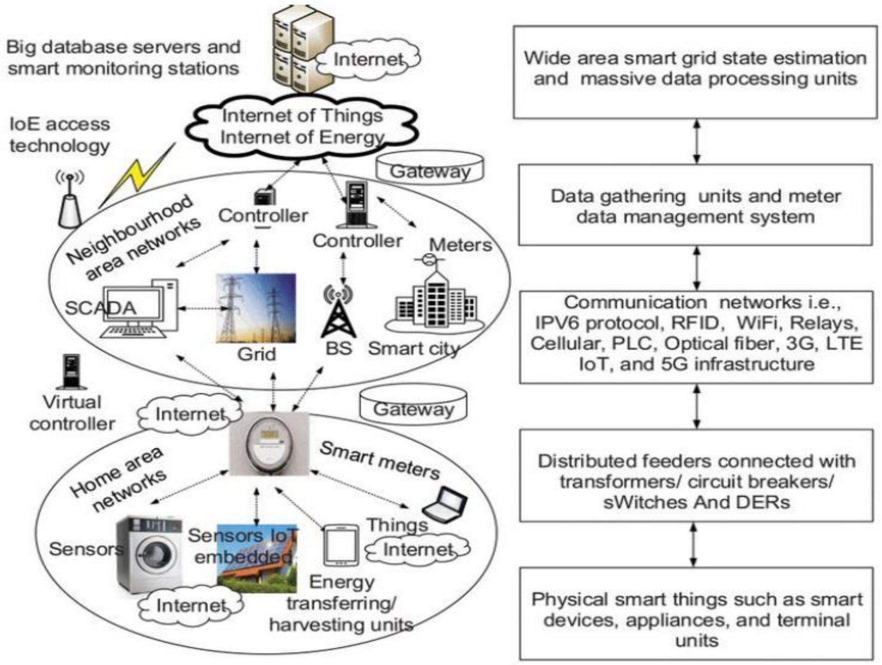

Big database servers and smart monitoring stations
Internet
Internet of Things
Internet of Energy
IoE access technology
Gateway
Neighbourhood area networks
Controller
Controller
Meters
SCADA
Grid
BS
Smart city
Virtual controller
Internet
Gateway
Smart meters
Home area networks
Things
Internet
Sensors
Sensors IoT embedded
Energy transferring/ harvesting units
Internet
Wide area smart grid state estimation and massive data processing units
Data gathering units and meter data management system
Communication networks i.e., IPV6 protocol, RFID, WiFi, Relays, Cellular, PLC, Optical fiber, 3G, LTE IoT, and 5G infrastructure
Distributed feeders connected with transformers/ circuit breakers/ sWitches And DERs
Physical smart things such as smart devices, appliances, and terminal units

Figure 2-2: IoE Communication Network Architecture [8]

As shown in Figure 2-2, the control centre can get the information from different sources and transmit it over IoT networks. Moreover, the IoT infrastructure guarantees the connectivity of the physical smart components. Thus, the IoT communication network handles the huge transmission and processing of information by enabling the bi-directional communication between them.

A second vision of IoT architecture is based on advanced technologies and use cases that have been suggested by Zhou et al. [9], as a reference they had the SGAM architecture [10], the local Area Grid concept, the FREEDOM system [11] and the framework of SG interoperability [12]. Figure 2-3 shows the second IoE design, which is made up of five layers.

1. Business layer
2. Use Case layer
3. Operation layer
4. Interface layer
5. Appliance layer

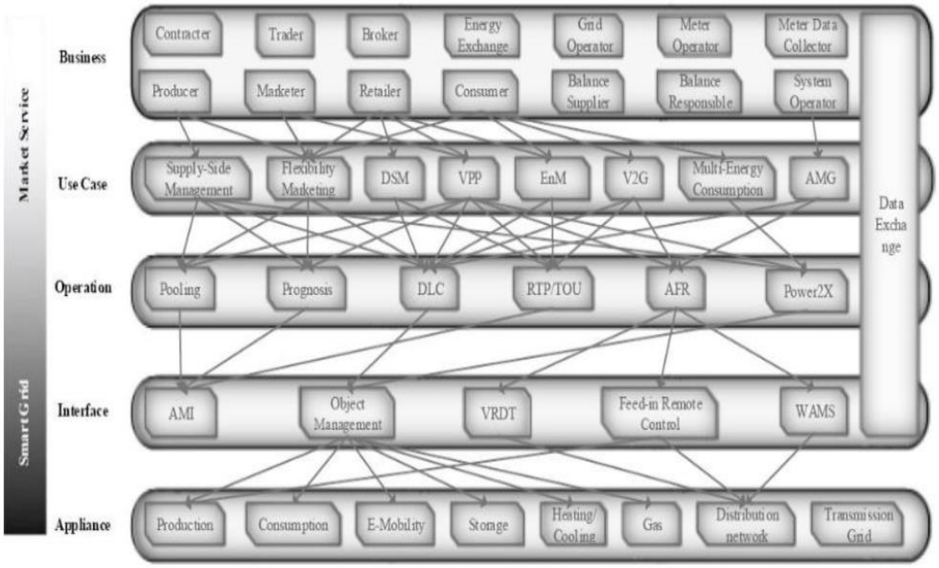


Figure 2-3 IoE Architecture [9]

The IoE architecture is composed of five layers starting from the business to the appliance layer going through the use case, operation and interface layers. The communication layer (exchange of information) is presented as a relay between the business and the interface layer passing via all the intermediate layers. To interact with other layers, the appliance layer requires a layer of interface, but it is not connected to Data Exchange. A portion of the operation layer, in addition to the interface layer and the appliance layer, delimits the Smart Grid, while the business layer, in addition to the use case layer and the other portion of the operation layer form the market services. Therefore, the IoE may be considered as a combination of SG and Energy services.

Each layer is made up of various components and roles assigned as follows:

Business Layer:

This layer comes from the liberalization of the energy market and treating energy as a service. Different roles and specialists are growing, which can be categorized as follows:

- Energy Trading: it cover production, usage, trading (sale and purchase) as well as SG maintenance.
- Real-time adjustment from production to demand: steady energy system operation.
- Distributed energy exchange: performing of energy exchanges (Trader), exchanging data between purchasers and dealers (Broker), energy transaction for small energy producer (Marketer).
- Information acquisition and data transmission for Smart Meter gadgets: deployment and maintenance of real meters (Meter Operator), meter measurements (Meter Data Collector).

Mention should be made of the ongoing partition of the energy market, with the result that new functions appear as billing agent and tariff management. In addition, a market operator can at the same time play several roles.

Use Case Layer:

This layer presents different exchange and interaction modalities between market roles within the Business layer. They can moreover have been considered as Business Models:

- **Supply-side management (SSM):** presents a set of measures taken to ensure efficient production, transmission and delivery of energy.
- **Flexibility Marketing:** this is a way for producers and retailers to transform unused electricity production into additional revenue.
- **Demand-side management (DSM):** involves the design and execution of activities planned to have an impact on the customer's electricity consumption in a way that will result in the necessary changes in the form of the utility load [13]. The DSM can be

executed within the Operation Layer via Real-Time Pricing (RTP)/Time of Use (TOU) and Direct Load Control (DLC).

- **Virtual power plant (VPP):** it refers to a decentralized grid, medium-scale power producing entities like Combined Heat and Power (CHP), solar and wind farms in addition to electricity consumers and batteries. By integrating a large number of Renewable Energy Recourses into the current energy system, the virtual power plant aims to reduce the load on the energy grid. The interconnection between the VPP components is sent via the central control unit, but they remain independent in their possession and operation. By interconnecting all participating components via a remote control unit, it establishes a data transmission between the control center system and the units involved. Therefore, the control center system is able to supervise, predict, and send the grid units [14].
- **Vehicle to grid (V2G):** the idea behind V2G is to allow plug-in electric vehicles to operate as distributed energy storage by providing demand-response services to the energy grid. The energy stored in the batteries of parked cars can be invested in such a way to permit the circulation of electricity between the vehicles and the distribution grid. The concept of the grid vehicle is comparable to the stationary power storage, but in the case of vehicles are the energy storage units. Therefore, vehicles are now able to participate and play a role in the stability of the electrical grid, such as providing the energy necessary to compensate for a disturbance. Simultaneously, they contribute to expanding the use of sustainable energy in the overall use of energy. The vehicle to grid can be achieved at the Operation Layer by three ways: Direct Load Control, RTP/TOU or Automatic Local Frequency Regulation.
- **Energy Management (EnM):** it is already deployed around the world. As indicated in the ISO 50001, Energy Management is known as "Group of interrelated or associating components of an association to build up energy strategy and goals and to accomplish those targets" [15]. This expression covers both the technical and hierarchical assets and data structures required for the deployment of Energy Management frameworks. EnM contributes to energy saving by monitoring, managing, controlling and saving energy in a building, enterprise or process and should consequently be addressed in the context of the Internet of Energy IoE. EnM can use Direct Load Control and Power-to-X in the Operation Layer.

- **Multi-energy consumption:** Multi-Energy Systems (MES) includes electricity eat, cooling, energy, transportation, etc., ideally collaborate with each other to enhance technical, economic and environmental productivity [16]. These systems can play a major role in the de-carbonization of the energy sector, in this way, adaptation to MES is of highly relevant to the concept of Internet of Energy.
- **Autonomous micro grid (AMG):** it is a system that operates independently by relying on the grid and the inner load situation, without the operator's involvement [17]. AMG can be achieved to different degrees, from continuous monitoring, fault diagnosis and self-healing, to automatic frequency and voltage guidelines, transformer control to DSM deployment and interaction between AMGs.

Operation Layer:

The functions that exist under this layer are necessary to realize the use cases that we have just described and mentioned in the previous section. The most important functions are listed as follows:

- **Pooling:** is to gather the distributed energy, storage, availability, flexibility or the demands of these to attain economies of scale.
- **Prognosis:** Energy supply and demand alerts caused by the intermittent supply of sustainable energy are essential for the operator to design how the network operates. Producers, Sellers, Aggregators and Dealers also need a prognosis to reduce the energy cost. The system and grid operator relies on the grid status prognosis for planning and performing maintenance.
- **Direct Load Control (DLC):** DLC technology allows utilities to turn on and off a specific set of particular household equipment's like air conditioners or water heaters during peak hours. DLC platforms in households have been widely tested and implemented in the US while in Europe the evolution and growth of DLC is modest due to the lack of regulation [18].
- **Real-time pricing (RTP)/time of use (TOU):** RTP and TOU address pricing plans where the cost and value of electricity changes over time to reflect the supply and demand balance. The only difference is that RTP provides consumers with data on the current electric energy

price at any given time while TOU only changes between a low fixed cost levels over a slight fixed period. Thus, consumers are encouraged to shift the load from peak time to valley time.

- **Automatic frequency regulation (AFR):** the AFR task is to automatically provide power in 0 to 30 seconds to adjust down the frequency of the power grid. These days, because of the emergence of sustainable energy resources, but the reducing of spinning reserves given by the generators, technologies like battery storage and V2G [19] are implemented to give AFR.
- **Power-to-X:** Power-to-X refers to different energy styles, which are the result of converting the power that cannot be used at the time of its production, like Power-to-Gas, Power-to-Fuel and Power-to-Chemical. An important study comparing the environmental impact of various Power-to-X was done in 2014, this study demonstrates that the highest deduction of global warming is made by Power-to-Heat, Power-to-Mobility and Power-to-Power. The lowest CO2 reduction value is obtained by Power-to-Power [20].

Interface Layer:

The functions of the operation layer are interpreted to commands and signals, which will pass to the Application via the Interface layer. Thus, component information is collected through the interface layer and transmitted to the function layer. The appropriate interface layer technologies are indicated as follows:

- **Advanced metering infrastructure (AMI):** AMI is a system that meters, collects, controls and evaluates the energy consumption at the demand site and transmits this information to utilities, grid operators and customers. An AMI system, as presented in Figure 2-4, consists of the below listing components:

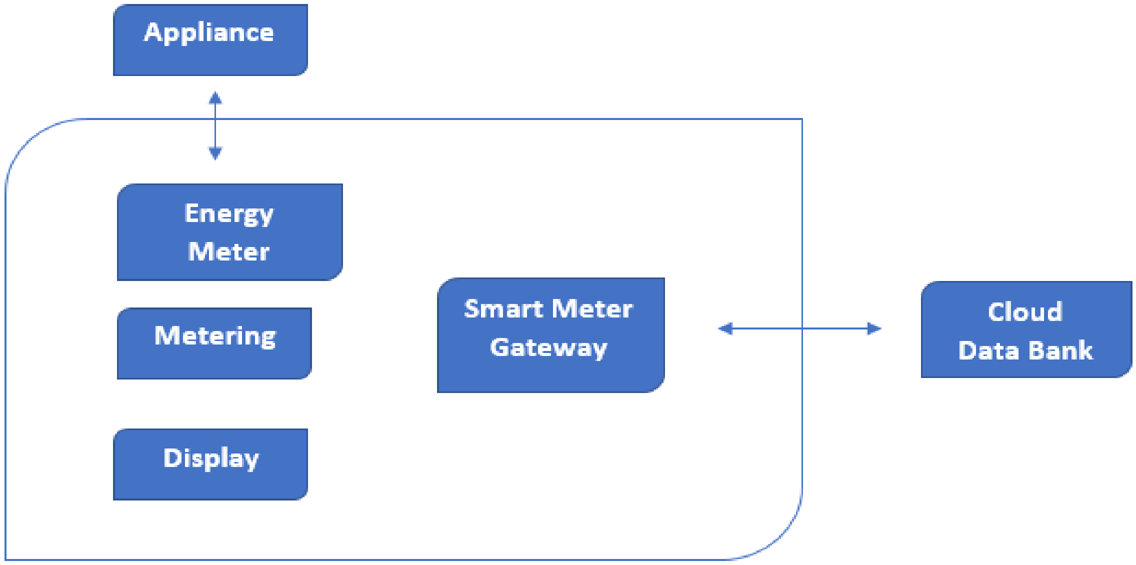


Figure 2-4: AMI Components [9]

- ✓ **Meter:** is responsible for energy consumption and generation real time metering and transmitting information.
- ✓ **Display:** is responsible for receiving and processing of information, and it shows the power usage analysis.
- ✓ **Energy manager:** it receives RTP/TOU or it is preconfigured to conditionally produce signals to control the devices and the condition of the equipment.
- ✓ **Smart meter gateway:** it is used to exchange information and signals with external and it links the components within AMI.
- ✓ **Cloud databank:** this is used to record and store the historical power information that can be accessed by externals and customers

AMI structure's complexity and simplicity depend on data security requirements, configuration and the connection infrastructure. Different agent can benefit from the AMI like:

- ✓ **Customers:** by visualizing and presenting the power utilization, these customers may achieve power and price savings.

- ✓ **Utilities:** saving human resources to collect and record data, proposing new value added services, improving the prognosis of demand.
- ✓ **System Operators:** it offers to operators a better knowledge of the grid status and conditions.

The AMI system has been widely deployed and implemented in Europe, the US and other countries. Within the restrictions that limit the spread of the AMI, we can name the technical problems, the information security and standardization, and the investment [21]. The three steps in implementing the AMI are summarized in Figure 2-5.

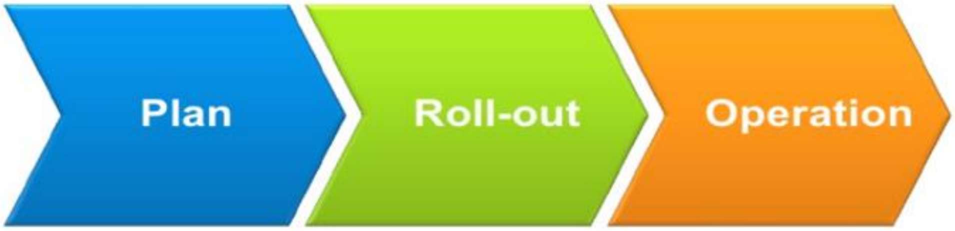


Figure 2-5: AMI Implementation Steps

- **Wide area measurement system (WAMS)/ phase measurement unit (PMU):** WAMS is a developed grid dynamic performance verification platform consisting of different Phase Measurement Units (PMU) and Phasor Data Concentrators (PDC), along with data devices, Global Positioning System (GPS) and operating infrastructure. The reason for the implementation WAMS is the collection of ,the sharing of coordinated control activities at high granularity and over the entire region, which lets the energy grid to be more efficient and reliable [22]. The idea for WAMS was suggested in the 1980s, and the primary exhibition project was sent to the US in 1995. However, WAMS is gaining its business used just throughout the past decade because of the Smart Grid orientation.
- **Feed-in remote control:** Via Feed-in Remote control, the sustainable power plants can be managed to reduce the energy generation or be completely turned off to avoid negative energy costs. The Feed-in Remote Control also provides better deployment and integration of sustainable power to the VPPS [23].

- **Voltage-regulated distribution transformers (VRDT):** VRDT automatically adjusts the conversion ratio to separate the voltages from the medium and low voltage grids. This results in a total abuse of the current transmission capacity and a deduction of the prices from conventional grid support [24]. VRDT implementations exist mainly in Germany, where the rapid growth and deployment of distributed solar power previously imposed on Grid Operators either to extend the electrical cables or to implement VRDTs.
- **Object Management:** an object-oriented software that examines the availability of the object and interprets the order from the Operation Layer to a group of signals in the control unit of a particular device or component.

Appliance Layer

The appliance layer includes all the physical facilities (such as solar panels, wind turbines, batteries, heat pumps) along the power chain involving power generation, transformation, transportation, delivering, storage and utilization. The power flows in the Appliance Layer are related to the exchange flows in the Business Layer. Appliances are managed via the Interface Layer by market roles within the Business Layer as use cases and operations.

We imagine that, the suggested structure shows a well-balanced review of the most well-known innovations, user cases, and market roles that make up and monetize the Internet of Energy. However, the IoE includes a wide range of technologies and applications, which can be studied and used by the teams of professionals concerned by themselves.

2. 2. 3 Internet of Energy Opportunities

The outcomes that the IoE brings along are varied:

Initially, the extended interconnection between all the agents of the power grid allows the exchange of information in real time and a better synchronization and optimization of their operations. As a result, the current passive power grid is shifting in a market- and service-oriented decentralized framework. In addition, another data and communication infrastructure is emerging that will ultimately link together decentralized energy sources to a multi-sources smart distribution grid [6].

In addition, the IoE supports the emergence of innovative power services, such as the optimization of energy use via Smart Meters, smart home management and control via IoT-based consumer devices. This will increase the chances of households, public sectors and small and medium sized companies to manage and adjust their energy demand and thus to minimize their energy prices by consuming energy during off-peak hours. With the Demand Side Response that allows SMEs and consumers to move their energy demand in real-time, a secure and affordable energy system can be guaranteed. In addition, the growing integration of sustainable resources into the energy grid will ensure a much better balance between power generation and demand and allow households to make additional profits.

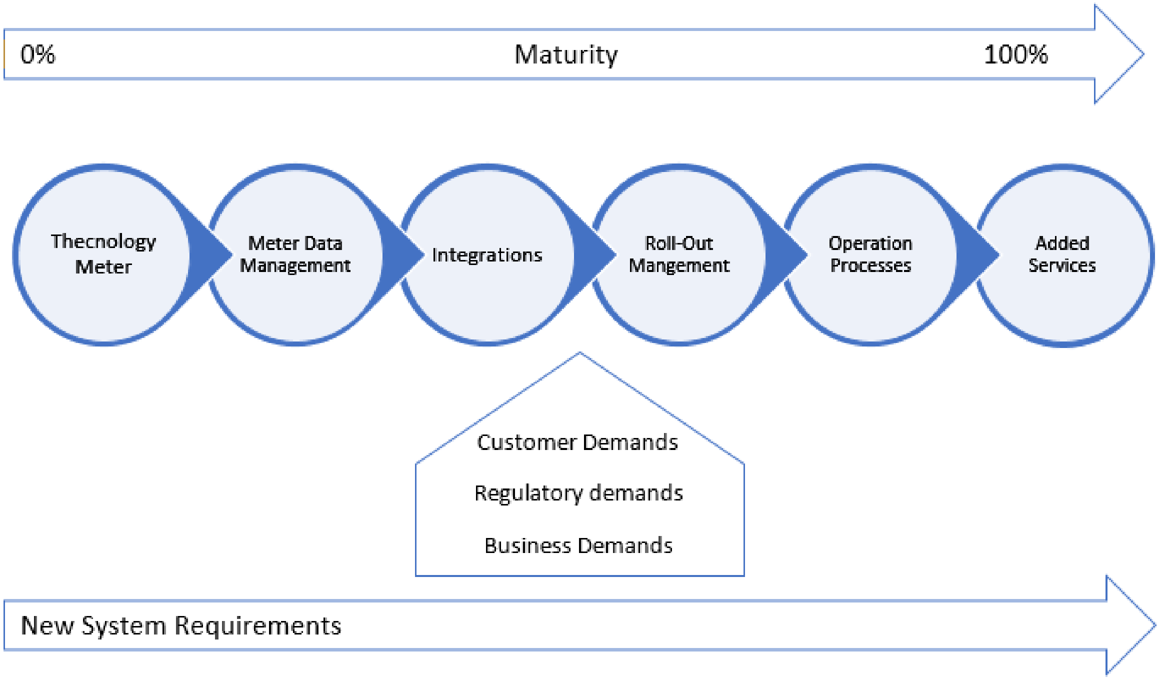


Figure 2-6: System Requirements to enable IoE

On the other hand, IoE facilitates the rise of the concept of prosumers who refer to a consumer who is capable of producing and consuming energy at the same time. Consumers have previously become expected prosumers by integrating a small scale power production unit like the solar panel on their roofs. In addition, the energy generated can be used by the producer himself or sold to the grid. In this case, the energy provider is then a buyer of energy. The prosumer can save the energy in a battery system or an electric vehicle, and is able to manage energy exports and imports by how it uses intelligent devices in their premises. From a technical perspective, these two ways of communication and power transmission between the prosumer and provider is facilitated by SM smart meters that, on the prosumer's site, show the use of prosumer power and equal costs at different time intervals and therefore display possible areas of savings whit lower power consumption. This will then allow utilities to offer their customers progressive and dynamic pricing (TOU tariff) and ensure the reliability of billing as a standard telecommunications practice.

IoE will positively affect the industrial support sector because of the ability to remotely detect and estimate any abnormal technical behavior in the network. Predictive Maintenance that depends on IoT technology is based on forecasting device failures and avoiding the happening of technical issues and problems. Therefore, the recurrence of maintenance missions and related expenses can be kept as low as possible.

2. 2. 4 Internet of Energy National Regulations

The IoE can also have a positive impact and bring important benefits at the national level which will help countries to control electricity demand and prevent outages in the future. Many nations have perceived the potential of this disruptive technology and have begun thinking about the best deployment plans.

- **United States of America:** The Future Renewable Electric Energy Delivery and Management (FREEDM) center funded by the National Science Foundation has developed a new power transmission infrastructure with “plug-and-play” capability and open-standard communication operating system.
- **United Kingdom:** According to assessments from Nicola Shaw, Executive Director of the UK's National Energy Grid, about 30%-50% of the fluctuations in the energy network in the UK could be corrected addressed when both companies and households control their energy consumption at peak times. The test for the national grid is to encourage and gain more organizations to adopt Demand Side Response technology (DSR) [25].
- **European Union:** As per Covrig et. al. [26], 459 projects on SG and IoE (covering research, development as well as review and implantation projects), were sent to all over EU and non-EU countries from 2002 to 2014. The amount of financing that was invested in such projects was around €3.15 billion, of which 50% came from France, the United

Kingdom, Germany and Spain. Denmark had the highest investment in this kind of projects. France and the United Kingdom had the highest average funding per project. Germany had the higher the highest number of projects and companies engaged. These projects focused on the production, delivery and use of user-centric energy and output, which correlated with the wider IoE concept. From 2008 and 2013 the "E-Energy" project that was financed by the German government and published by the Federal Chancellor Angela Merkel as beacon projects, has as a direct target the creation of IoE in six different regional models via the development of a highly efficient and environmentally friendly ICT-based power system.

According to the European Commission directive released in 2006 by Brussels, each member of the EU is obliged to participate in the implementation of Smart Meters and to move 80% of its inventory of traditional meters to smart meters by 2020. Each nation may have its own system and infrastructure model and at the time act in accordance with the national law.

But, implementing of the instructions changes from nation to nation. Some nations are extremely optimistic about the implementation and use of the smart meters. Therefore, on 1st of December 2018, France started implementing smart meter across the country. The target is to achieve the 95% smart meter implementation benchmark by 2020. French electric grid manager Electricité Réseau Distribution France (ERDF) will supervise the rollout of 28 million of the French smart meters, which represents 80% of the total 35 million meters in France, where the Linky and third party can reach the metering information. The estimated energy savings for households are set between 5-10% [27].

Various countries have chosen not to deploy the smart meters on a national scale. Between the causes that make it difficult to deploy smart meters across the country, is the lack of awareness of residents regarding this technology and the serious cybersecurity concerns of businesses can be mentioned.

2. 2. 5 Internet of Energy Challenges

As already mentioned, the huge deployment of Iowa's strategies and policies occurs with a significant delay due to different challenges that can be divided into three categories as follows:

1. Technical challenges

Initially, the IoE should emerge from a highly sophisticated network, which will integrate embedded systems such as smart energy grid, distributed sustainable resources, sensors and need a decentralized near real time verification and control and management of big data sets from different components. In addition, the sporadic nature of sustainable production and the variability of loads enable an extremely difficult smart energy management system to be achieved [28]. Therefore, providing a sustainable energy supply for critical loads remains an important challenge that could be solved by an efficient demand-side management. An additional challenge is the regulating of the voltage and frequency of the power grid within the framework of strict standards for smart grid [29].

2. Cyber Security Challenges

The Integration of internet technology with smart grid networks mains that we are opening up utility infrastructure to the risks and hacking issues and interference. Therefore, cyber security issues are one of the major threats to IoE technology. The three major cybersecurity performance objectives are:

(i) Secure data access and use

(ii) Data Integrity

(iii) Confidentiality, privacy, and data proprietary [30]

Previously, there were various severe cases of cyberattacks on the grid. The most critical attack was in the Bushehr nuclear power plant (Iran) which targets the SCAD system that was used by hackers to monitor and control the power grid [31]. Hacking into power generation equipment, delivery and the control station as a target could lead to a dramatic grid outage or damage to infrastructure. To face this type of challenges, specialists provide authentication, integrity protection, and encryption [32].

3. Business Challenges

The business model of the conventional power grid depends on a huge centralized utility and generators enterprises with a huge market share, from production consumer homes. The shift in power paradigm allows, as already mentioned, the improvement of a new business model and services, which, however, can't be completely implemented for technical reasons: IoE infrastructure and regulatory framework system are still in their early stages. Removing of regulation and transforming today's electricity market are the main challenge to achieve an upcoming service-oriented power market [33].

In the next part of this chapter, we have grouped together a more distinguished overview of the selected European countries concerning the state of IoE, particularly in Germany and Greece. The selection of these nations is due to their participation in the development of the energy sector, in particular in Germany where they developed and implemented their own advanced SMGW based system on.

The German SMGW architecture was a taken as the reference architecture in our study where our main purpose is to develop a similar open-source system that can be used and designed by other countries and researchers.

2. 3 IoE in Greece

2. 3. 1 IoE Awareness

From a brief examination of the Greek electricity supply, we can conclude that the two main fuels are oil and coal, while “environmentally friendly" natural gas was inserted in the 90's and increased remarkably in 2011 before going down again in 2016. During the same period, coal-based production also decreased, so that residual energy generation comes from sustainable energy resources, where the biofuels and waste generation make up the majority, then it comes solar panels, hydro and wind [1]. Therefore, it is becoming clear that Greece has implemented environmentally friendly energy generation and supply, responding to the European Union policies and measures that have been implemented. But to date there is still no clear long term strategy, however the nation joined the 2050 energy roadmap in 2012. [1]

Today, when it comes to IoE the data and awareness are still insufficient. It is possible that some Greek enterprises are working on the process of implementing this new technology or shifting to less fuel energy resources and less dependent plan. At present there is not a great deal of data on this subject, but the energy and the environment present one of the first eight areas of concern of the Greek strategy for study, research and innovation, which includes seven sectors

1. Power Efficiency
2. Power generation from sustainable resources

3. Power technologies for agriculture
4. Power storage
5. Hydrogen and fuel cells
6. Energy Smart Grids technologies
7. Fossil fuel effect deduction.

These areas are normally made up of different sub-sectors, each of which requires massive research and development for future deployment [1].

2. 3. 2 IoE Future in Greece

As mentioned above, it has been shown that it is so difficult to handle a future IoE scenario for Greece, since this new technology is not yet completely introduced as a concept and application in Greece. But, as already mentioned the Greek Ministry of Environment and Energy in 2012 suggested a national energy strategy roadmap till 2050, which sets specific objectives for Greece's energy future as follows:

(i) Integration of sustainable energy by 60% to 70% of the total energy consumption by 2050.

(ii) Stabilize power through energy saving measures.

(iii) Development of a decentralized generation units and a smart energy grid.

2. 4 IoE in Germany

2. 4. 1 IoE Awareness

In 2008 and for the first time, the Internet of Energy word IoE appeared in Germany at the level of the Federal Ministry of Economic Affairs and Climate Action known as BMWI. Back in the time, Germany’s electricity supplier sector has faced major challenges related to the environmental change, the rapid increase in energy demand, and the decline in natural sources, as well as the enormous development and growth of disruptive technologies such as the Internet of things IoT and advanced computing. In addition, the technical components of the electrical infrastructure must be upgraded and replaced by new production, transmission and use elements. At the same time, the power plants producing about half of the total production in Germany were almost out of service and at the end of their technical life. At the same time, a large-scale renovation needs to be attempted in almost 33% of German residence to implement a new system of energy saving system and communication equipment [1].

It was recognized that the gap between the energy sector and Information and Communication Technology (ICT) should be completed to obtain an environmental and economic energy production for both the public and private sectors. Therefore, the target was set to inspire IoE - a digital network, which intelligently controls, manages, and regulates the power grid.

This approach was implemented through a very large and pioneering national E-Energy project which has been published by the BMWI in cooperation with the environmental federal Ministry between 2008 -2013. This project aimed to develop a new decentralized electricity market system and to test these new processes in real-life cases in six German regions. Figure 2-7 shows the geographic program distribution.

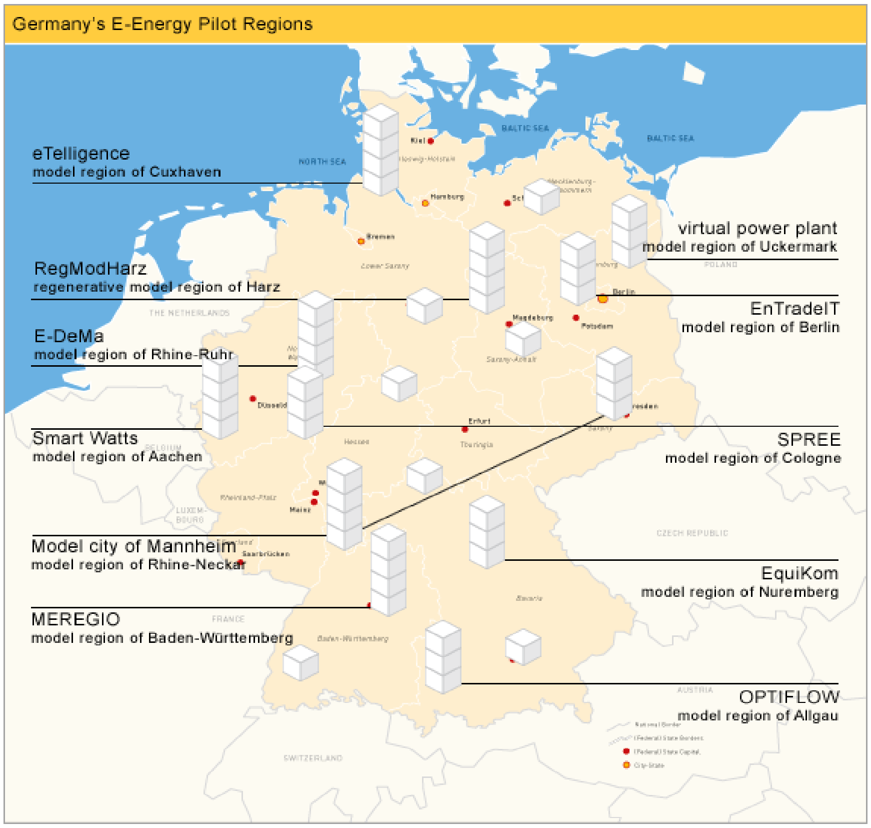


Figure 2-7: Germany's E-Energy Pilot Regions [34].

This project developed new ICT products, processes and services that will help in improve the energy efficiency, secure energy supply and overcome the nature change.

The E-Energy project also proved that there is a chance for new business models in a new field at the crossroads between the energy and ICT industries.

2. 4. 2 Germany Smart Metering

By giving great importance to standardization and security, the German concept of smart metering is based on two main components: the Smart Meters and the Smart Meter Gateways (SMGWs), where the merging of both introduces the Intelligent Metering System (Intelligentes Messsystem) [35, 36]. The SM by itself is an advanced digital energy meter capable of providing near real time energy measurements, and it is an equipped with a display to visualize the power value at various time intervals. However, the SMGW is the communication component, which has two main roles: firstly, communicates SM's energy measures to External Market Participants (EMP) and secondly, allow the EMPs to send commands back to the local control boxes in order to adjust the load. External Market Participants are divided into two categories active and passive, where passive EMPs receives only energy metering measurements or derived information, and active EMPs can transmit commands to local control boxes [37].

Later on, Smart Meters will be mandatory for installations, and referring to Germany's Metering Point Operation Law ("Messstellenbetriebsgesetz", MsbG) [35] the deployment of SMGWs continues a strategy of progressive deployment until 2032, making it mandatory at the end for consumers of more than 6000 kWh/year, or for users with sustainable feed-in is about 7 kWpeak and above. However, for users whose consumption is under these thresholds, the deployment of SMGW is not mandatory, therefore, the possibility of an automatic Smart Meters measures the transmission to external entities or the receipt of load shifting commands from external entities. Figure 2-8 shows the SMGW rollout schedule in Germany

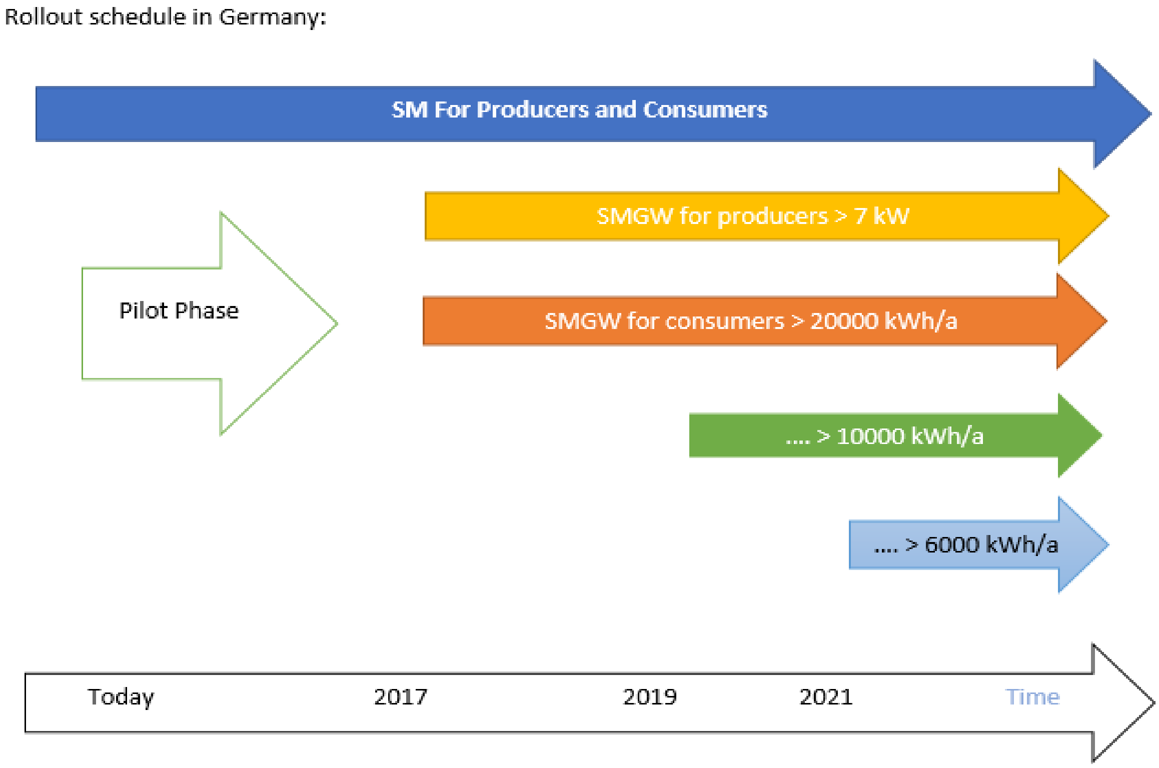

Rollout schedule in Germany:
SM For Producers and Consumers
SMGW for producers > 7 kW
Pilot Phase
SMGW for consumers > 20000 kWh/a
.... > 10000 kWh/a
.... > 6000 kWh/a
Today
2017
2019
2021
Time

Figure 2-8: SMGW Rollout Schedule

2. 4. 3 Germany Smart Metering Legislation

The European directive 2009/72 EC was adopted by the European Parliament, this directive obliges the European Union's nation to deploy smart metering infrastructures, only when a positive macroeconomic assessment is recognized [38]. In the case of Germany, the evaluation of the different deployment scenarios has been carried out and shows positive results in 2013. Therefore, in 2016, the German law on the digitization of the energy transition ("Gesetz zur Digitalisierungder Energiewende") [39] was published, it includes various modifications of the current laws and regulations, and introduces the new German law Metering Point Operation Law ("Messstellenbetriebsgesetz," MsbG). The MsbG deals with the installation and operation of smart metering system, provides a high level of data protection and it security, in addition to the use of protection profiles and technical guidelines to ensure security and compatibility of IT devices. The MsbG specifies the regulations for the compulsory deployment of intelligent metering systems ("Intelligente Messsysteme," iMSys) [40]. the iMSys can be considered to be the German version of an advanced meter infrastructure (AMI). As previously mentioned, it is composed of the SM and the SMGW. By law (§30 MsbG), deployment starts with the availability of iMSys from at least three different industries meeting all requirements, but by February 2020, this condition is met [41]. As previously mentioned, the SMGW plays the role of a relay to fill the gap between the local devices and the external entities that need to have access to these devices for example for billing purposes. To do this, the SMGWs is equipped with three different interfaces in three different communication networks and features to process metering data. Access to metering data depends on how the SMGs are configured [42].

2. 4. 4 Germany Smart Metering Architecture and Key Entities

1. iMSys has three major roles: Receiving, handling and transporting metering information to authorized systems
2. Developing metering information for consumers and technicians
3. Communication interfaces for deployment of value-added services such as SG and demand response, where demand response generally typically requires forwarding control and transmitting commands to DERs. Since the DER usually don't generally have the necessary interfaces to interact with the SMGW infrastructure, then an additional local communication device must be implemented. These devices are like control boxes, which are used to transmit and translate messages between different protocols, or energy management systems, which optimize the energy consumption.

2. 4. 4. 1 Intelligent Metering Systems Components

iMSys is the German version of the AMI, and it consist of smart meters (SM) and smart meters gateway (SMGW). Below is an overview of the iMSys system from a fully functional perspective. Figure 2-9 shows the various components of iMSys.

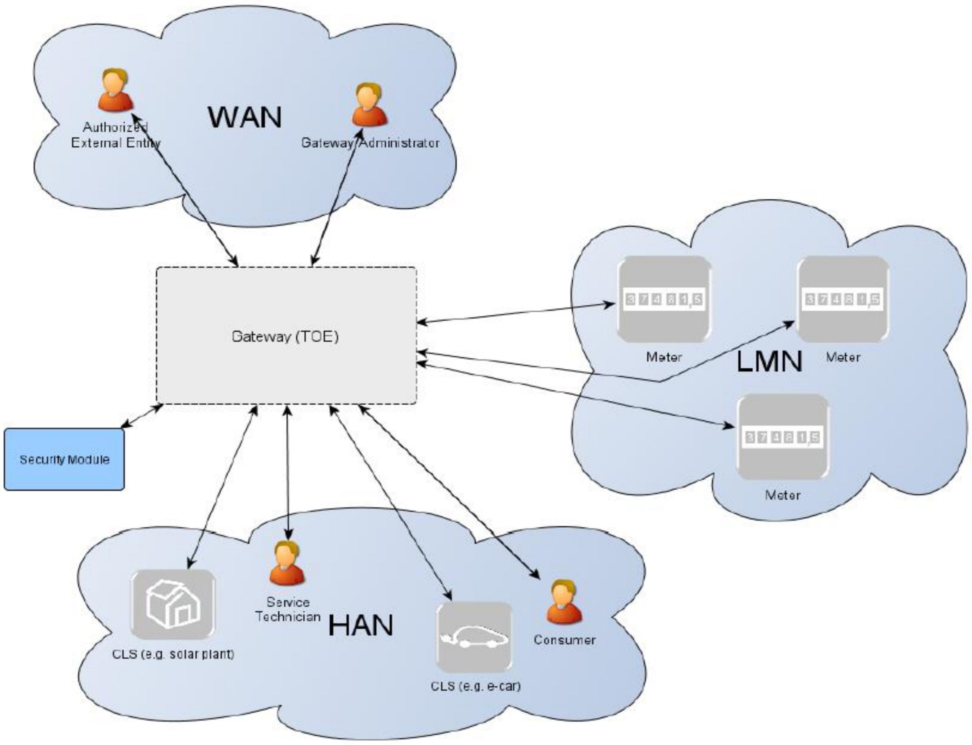


Figure 2-9: iMSys Functional Units [43].

The **gateway** plays the role of a relay to ensure a communication channel between the devices in the LAN, where we have the Home Area Network (HAN) and Logical Metrological Network (LMN), and the external entities in the Wide Area Network (WAN). Within the HAN network are generation plants, DER, control boxes that is called the Controllable Local Systems (CLS), however the LMN includes all connected meter units and finally the WAN is used for communicating with external entities (like Smart Meter Gateway Administrator" (GWA), and the "External Market Participants" (EMP). It can be considered to be firewall with smart metering functionalities. It also collects, processes and stores metering data and provides access to this data only to authorized entities. Before transmitting metering information, these data are encrypted and signed by a **Security Module** implemented at SMGW level. Usually SMGW uses cryptographic services provided by **Security Module (like smart card)** to secure the data and assets storage**.** In LAN this gateway also provides authorized users with an interface to access their relevant data and diagnostic data to the technicians.

Typically, an SMGW is deployed at the consumer premises of the commodity and allows access to local smart meters and also it allows access to the Controllable Local System (CLS) like power plants or smart home appliances. The SMGW is developed with a fail-safe design that ensures service continuity in case of any malfunction. In fact, there are different possible designs of SMGW which are shown in Figure 2-10, Figure 2-10 and Figure 2-12 as follows:

1. Gateway and multi-Meters: where this SMGW can communicate with one or more meters in LMN, and has two other interfaces that are connected respectively to the HAN and the WAN

2. One box Solution: where the gateway and the meter are implemented together in a single physical entity and ensure the functionality of both. Usually such type can be deployed in large premises where all energy meters are implemented in the same cabinet.

3. Gateway with external communication devices: Figure 2-12 confirms that the overall design and operation of SMGW has some basic features, but does not require the gateway safety aspects. These functionalities can be deployed via external devices that do not belong to the SMGW.

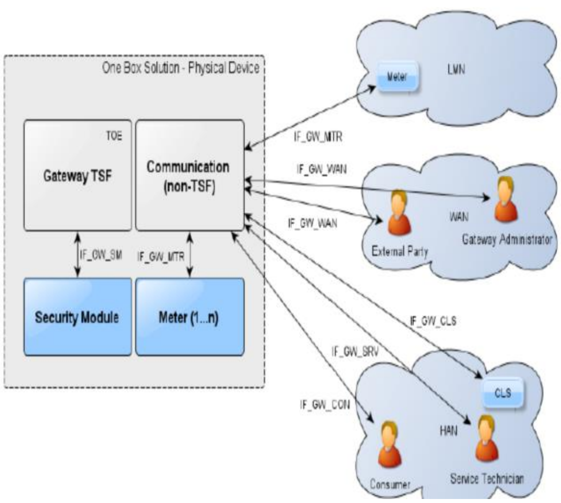


Figure 2-10: Gateway and multi-Meters [43]

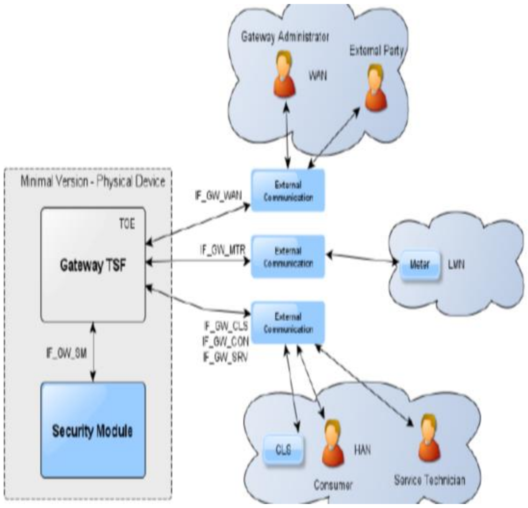


Figure 2-11: One Box Solution [43]

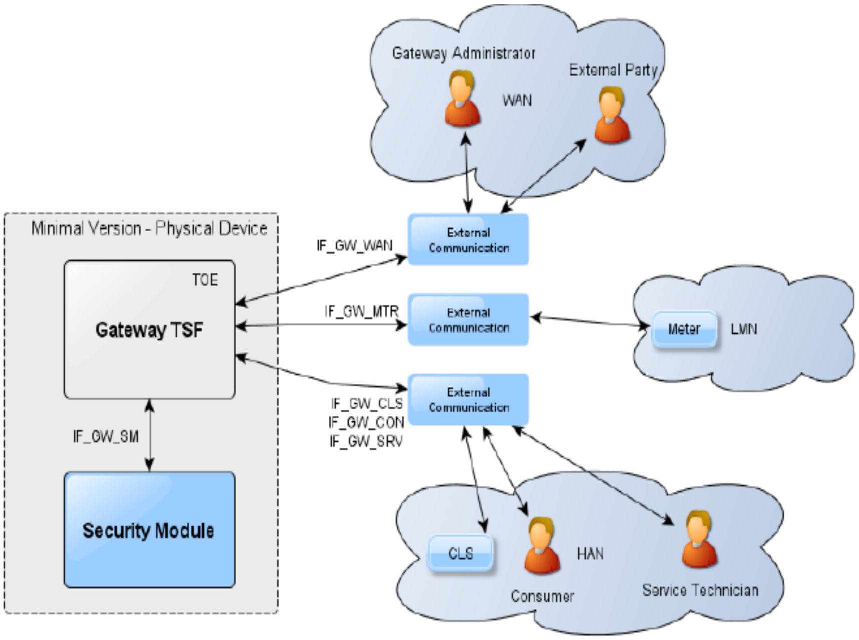


Figure 2-12: Minimal Implementation [43]

The **Meter** is responsible for recording the use and generation of one or more services (such as power, gas and water) and upload these data to the SMGW at predefined time intervals. To ensure the security requirements (confidentiality, authenticity and integrity), this data must be signed and encrypted before being transmitted. The Meter is similar to traditional meters and has specific security requirements, it will be locked as conventional meters as indicated in the guidelines of the calibration authority. On the other hand, the connection between the meter and the gateway is secured with encryption and integrity protection measures.

Controllable Local Systems (CLS) may range to cover local electric energy generation plants, control loads like smart home appliances and home automation platforms. The CLS uses the communication services provided by the gateway, but it is not considered as part of the iMSys.

Smart Meter Gateway (GWA) has the role of a trustworthy authority for the smart meter gateway. Each SMGW is allocated to a GWA. GWA is the only authorized entity which is responsible for the configuration and execution of administrative functions (such as firmware updates) on the SMGW using the "management channel", where this channel is set by adopting the so called "wake-up service". To play out this role the GWA can safely speak to the SMGW by establishing this channel.

External Market Participants (EMPs) represents all other entities that communicate with the SMGW from the outside or the WAN. Usually, they differentiate between active and passive EMPs where passive EMPs only receives metering information, however, active EMPs noted aEMPs are allowed to interact with one or more CLS in the HAN, using the SMGW transparent data tunnel. Consumers are those authorized parties for which the use of energy is measured. The SMGW is capable to differentiate between various consumers, to maintain their privacy. Each consumer is authorized to access their own metering data and can retrieve them via a specific interface from the SMGW or metering unit. For maintenance and support, technicians have local access to the SMGW through the HAN.

2. 4. 4. 2 SMGW Configuration

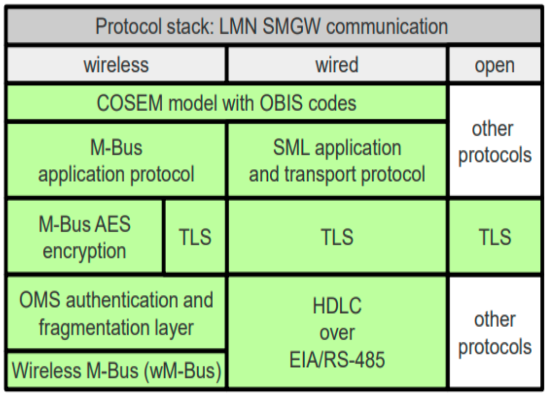
The SMGW functionalities are divided based on the network area LMN, HAN or WAN and the defined use cases. On the other hand, the communication profiles are configured and implemented on the basis of specific use case also, where each communication scenario requires specific requirements.

If we take the WAN use case "administration and configuration" which is reached by managing WAN communication. Moreover, if we take the tariff use cases that describe the bases that specify which data should be measured, recorded, the time interval between measurement, the manner in which such data should be processed, and the timing and sender of such data.

There are various types of configuration profiles, to meet all those requirements. The WAN and HAN communication profiles define the parameters to communicate with the SMGW in the corresponding communication networks, for example a meter profile is used to set the communication between the SMGW and the meter itself, where the evaluation profile is used to process metering data and a proxy profile is used to connect the WAN and HAN communication profiles to define which DER and EMPs are allowed to use the established data tunnel between WAN and HAN. [6]

SMGW used a variety of communication protocols based on the network area. Each interface has its own protocol stack, so therefore there are three different stacks that will listed as follows:

SMGW: LMN Communication: this the interface between the SMGW and the Smart meter where the protocols in use are presented in Figure 2-13: mainly COSEM over M-BUS in case of a wireless media or COSEM over SML (specific for Germany) in case of wired media is used. To ensure data security during transmission the TLS or M-Bus AES encryption protocols are implemented.

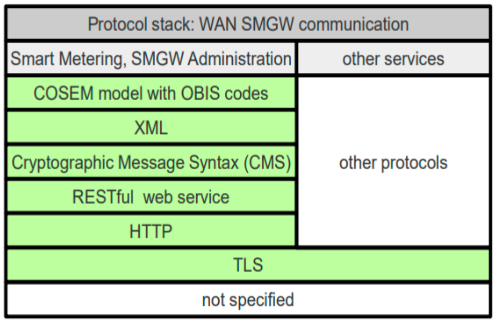


<table>
<tr><th colspan="4">Protocol stack: LMN SMGW communication</th></tr>
<tr><td colspan="2">wireless</td><td>wired</td><td>open</td></tr>
<tr><td colspan="3">COSEM model with OBIS codes</td><td rowspan="2">other protocols</td></tr>
<tr><td colspan="2">M-Bus application protocol</td><td>SML application and transport protocol</td></tr>
<tr><td>M-Bus AES encryption</td><td>TLS</td><td>TLS</td><td>TLS</td></tr>
<tr><td colspan="2">OMS authentication and fragmentation layer</td><td rowspan="2">HDLC over EIA/RS-485</td><td rowspan="2">other protocols</td></tr>
<tr><td colspan="2">Wireless M-Bus (wM-Bus)</td></tr>
</table>

Figure 2-13: LMN Protocol Stack [49].

SMGW: HAN Communication this is the interface between the SMGW and the CLS, for this interface there is no specifications defined by the TR-03109, however the security is provided by the TLS protocol.

SMGW: WAN Communication this is the interface between the SMGW and the external entities EMP usually the protocol that are used for this communication channels are HTTP, RESTful web service as shown in the below stack Figure 2-14, however the security requirements are provided by the TLS



<table>
<tr><th colspan="2">Protocol stack: WAN SMGW communication</th></tr>
<tr><td>Smart Metering, SMGW Administration</td><td>other services</td></tr>
<tr><td>COSEM model with OBIS codes</td><td rowspan="5">other protocols</td></tr>
<tr><td>XML</td></tr>
<tr><td>Cryptographic Message Syntax (CMS)</td></tr>
<tr><td>RESTful web service</td></tr>
<tr><td>HTTP</td></tr>
<tr><td colspan="2">TLS</td></tr>
<tr><td colspan="2">not specified</td></tr>
</table>

Figure 2-14: WAN Protocol Stack [49]

2. 4. 5 Germany Smart Metering Security

The special feature for the German AMI is the SMGW as a secure communication unit on the user's premises. As already mentioned, the main role of such devise is to collect, save and process metering data in addition to applying certain tariff rules before being transmitted to authorized entities. SMGW has three security zones: LMN, HAN and WAN each security zone has specific features. The LMN shall establish communication between the meter and the SMGW, but to communicate with authorized EMPs the SMGW must be equipped with a security module hardware who is in charge of data encryption and signing before being transmitted. Both the SMGW and smart meters refer to the iMSys and the digital smart meter refers to a modern metering unit.

2. 4. 5. 1 SMGW Secure Bidirectional Communication

The most undervalued fundamental service of the AMI is the ability to build a secure communication tunnel to CLS at the user side. The established transparent data tunnel can be used for other services than the transfer of metering data to the EMP and configuration by GWA. This is the main characteristic that will be used to design value added services such as smart grid application and P2P energy trade. By establishing this transparent secure tunnel, a bidirectional communication will be established between the CLS in the HAN and the EMPs in the WAN via the SMGW. The use of this feature differentiates the active EMP from the passive EMP where the passive EMP only receives data and is not allowed to interact through the transparent tunnel. There are three HAN communication scenarios between the CLS and aEMP: HKS3, HKS4, and HKS5.

These scenarios differentiate in who is in charge for establishing the data tunnel. Communication profile configuration is required for each CLS and aEMP to create a transparent tunnel through the SMGW. This profile contains different parameters, including the IP address the port number, the communication scenario, the SMGW interface, the TLS certificate for the involved players and time specifications like the maximum active session time knowing that the duration should not exceed 48 hours otherwise, the SMGW should remove the session and the communication profile. [44] In other words, the tunnel should be reestablished at least each second day. Moreover, a proxy profile is required for the three HAN scenarios HSK3-5, this profile is a reference for the HAN-WAN communication profile and defines additional data based on the scenario requirements. The data tunnel is initiated at the end nodes defined in the proxy profile and mentioned in the communication profile. In the following, a detailed description of the HKS3–5 is presented:

HAN Communication Scenario HKS3: in this scenario and by using the SOCKSv5 protocol, the CLS starts the initiation of the tunnel. It uses a proxy server application where the CLS is the client and asks the SMGW (plays the role of a proxy in this case) to communicate with the aEMP. TLS for SOCKSv5 protocol is adopted for authentication. The whole TLS communication is then included in SOCKSv5 messages. In WAN the SMGW plays the role of a TLS client while the aEMP is considered as TLS sever [45, 46]. There are various requirements that have to be met before establishing a connection.

1. SMGW has to be configured using both communication and proxy profiles
2. Proxy profile and the connection requested parameters configuration has to match, in such a way that only the defined CLS can request a data tunnel and can only connect to an aEMP already defined in the profile
3. The connection can only be established if both CLS and aEMP have a valid TLS certificate that meet the SM-PKI requirements and technical regulations.
4. SMGW must have both a HAN and WAN TLS certificate with the required private keys.

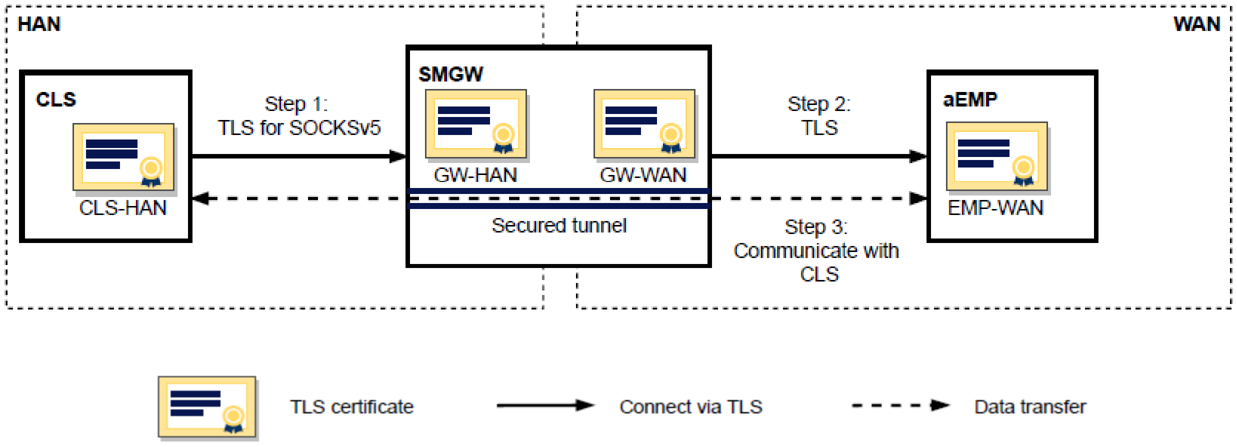


Figure 2-15: HKS3- HAN Communication Scenario [42]

HAN Communication Scenario HKS4: In this scenario the aEMP starts the initiation of the tunnel. While only the GWA is able to communicate with the SMGW from the outside, aEMP requires the assistance of GWA to communicate with the SMGW in order to establish the tunnel connection. Thus, as a first step the aEMP communicate with the GWA, in case the SMGW is not connected to the GWA, a wake-up signal is sent and used to establish a TLS connection (it is important to mention here that there is no normalized interface to communicate with the GWA). Once the connection is established, this means that the management channel is in place therefore the GWA is now able to send the data tunnel establishment command. This command refers to a proxy profile where the connection parameters are defined for both the CLS and the aEMP. in this case, the SMGW acts as a TLS client in both the HAN and WAN areas and is also responsible for starting the TLS connections. On the other hand, CLS and aEMP are obliged to act as TLS servers and hear the connections. For security requirements, and for communication encryption the SMGW, CLS and aEMP must have a valid TLS certificate from the SM-KPI and compatible private keys. Figure 2-16 shows different steps for establishing that connection.

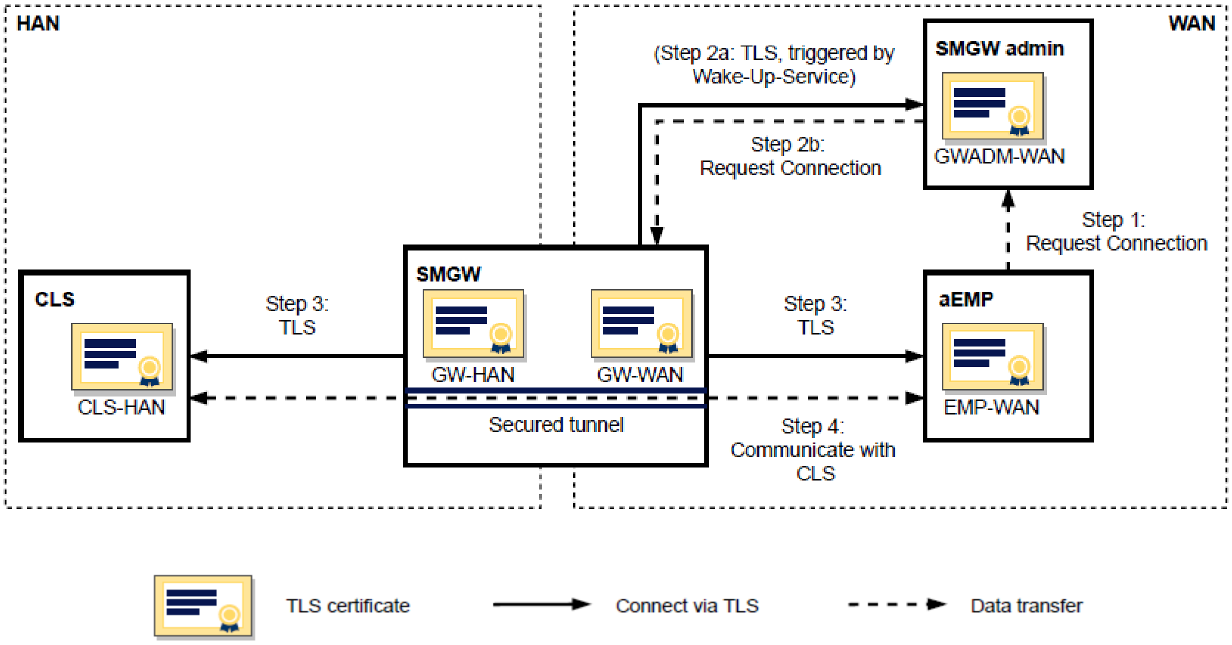


Figure 2-16: HKS4- HAN Communication Scenario [42].

HAN Communication Scenario HKS5: in this scenario, it is the SMGW that initiates the connection. The event behind the start of the connection could be time or any event**.** Once triggered, the SMGW imitates two TLS connections one to the CLS and the second one to the aEMP. Here also, the SMGW acts as a TLS client foe both the CLS and aEMP. Figure 2-17 shows the different steps to establish such connection.

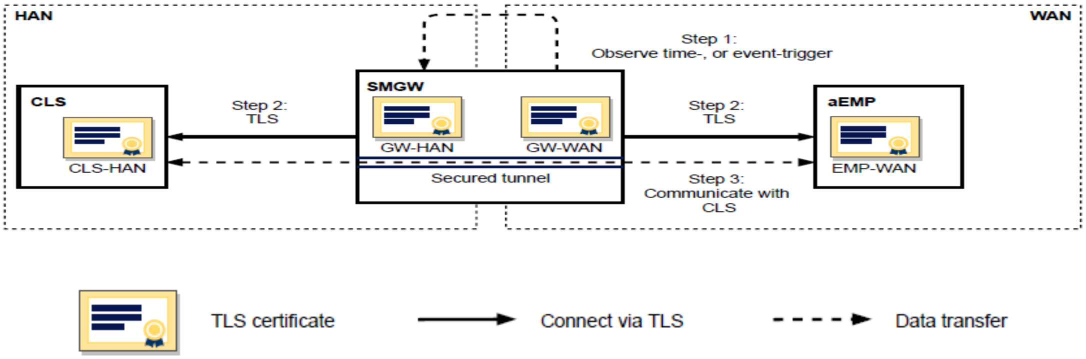


Figure 2-17: HKS5- HAN Communication Scenario [42].

We can see that the difference between the three scenarios lies in who is responsible for initiating the secure communication data tunnel.

2. 4. 5. 2 SMGW Secure Communication Architecture

Not only should the technical challenges and needs of the SMGW infrastructure be presented and taken into consideration, but also the huge security requirements should be also mentioned. The overall communications infrastructure of the WAN relies on the SM-PKI that is described in [45, 46]. The SM-PKI architecture and certificate plan used in the PKI are described. The whole architecture is composed of three hierarchical levels:

1. Root-certification authority (CA) as confidential reference
2. Sub-CA responsible of end entities certificates issuing (SMGW, GWA and EMP). These certificates ensure secure communication, data integrity and privacy. Thus, the published certificate of each end device consists of three other certificates with different objectives
    - TLS certificate to secure the communication channel
    - The encryption certificate is used to encrypt data independently of the TLS protocol.
    - A signature certificate this is used to ensure data integrity separately of the TLS authentication

For the WAN scenarios, the three certificates mentioned are required, while the TLS is required for the data tunnel. However, the SMGW has two versions of certificates:

1. The seal certificates, issued during the SMGW production process and it is stored on the security module
2. Before putting the SMGW into productive mode, they should be replaced by new certificates issued by the Sub-CA that define the role of the SMGW.

The main requirements for releasing SM-PKI certificates are illustrated in [46], covering the technical and personal aspects. The rules differentiate between active and passive EMP, with a high level of security for aEMPs. On the other hand, the TR-03109-3 has to be considered because it defines the cryptographic functions. It is important to mention that the SM-PKI does not include the HAN communication but cryptographic needs cover both the HAN and WAN communications. Especially the use of a set of elliptical curves and a restriction to five particular cipher suites for the TLS handshake is crucial. However, for experimental targets, the BSI has specified a second SM-PKI version with less security restrictions called SM-Test-PKI

This SM-Test-PKI is used to validate interoperability of the technical system with the SM-PKI.

2. 4. 6 Germany Smart Metering System in Comparison With Other Countries Systems

The deployment of Advanced Metering Infrastructure varies widely between nations. For the European Union members, an AMI comparison was conducted [47]. In addition to other elements, deployments differ with respect to features and interfaces, anticipated implementation strategies (fractional rollout versus full rollout), market design, deployment target rate, implementation period, projected expenditures. However, the German version with a powerful and highly regulated Smart Meter Gateway with the meter can be considered a unique system in comparison with other nations [48]. In general, data related to the privacy debate between 2010 and 2016 are presented, calling attention to the crucial features of smart metering in Germany's including SMGWs. due to the requirements which are specified and validated by the BSI as German authority and due to the national legislation, it is adapted to the German market. However, the whole idea, technology, and deployment of the SMGW as a gateway to secure the communication between the different areas HAN, The LMN and WAN could be applied to different nations, where nations adjust their national legislation accordingly. For example, the Swiss Federal Office of Energy has assessed the adequacy of various smart metering programs by specifying minimum national requirement and matching them to other systems deployed in other nations, resulting in a huge similarity between the Swiss needs and the German approach. Another comparison of countries smart metering systems is provided by the Austrian Energy Agency this report comparison covers the whole strategy and legislation basics.

2. 5 Conclusion

In this chapter we have introduced the concept of the IoE, this new technology is well defined and presented as it is currently the situation in the EU countries. Several architectural concepts have been described. On the other hand, the main challenges facing the rollout of this new technology are detailed and divided into three categories as already mentioned.

IoE's current situation in European countries is described in terms of the legislation and the infrastructure needed to enable technology in addition to smart technologies (SM) deployment strategies.

In the second part a detailed study of the German system was carried out, including the system architecture, the functions of the components, the specific German legislation and regulations and finally the security requirements. The implementation of SMGWs in Germany began in February 2020, after the European Parliament insisted in 2009 that smart meters be mandatory. The German SMGW is a certified communication device that allows secure communication between internal components of the power system components like meter, CLS and external entities like EMPs. Based on the German rollout strategy the standardized SMGWs will be widely available in the near future. Despite the fact that SMGWs are exclusively developed for the German system, they can be have a significantly taken into consideration by other international countries, because of their particular characteristics, and in particular high security standards. Based on this standard architecture that we have taken as a reference architecture in my thesis work while designing, configuring and testing our gateway prototype. A proof of principle for the realization of an open source and low-cost gateway that is capable of establishing a communication between the meter and the external parties.

Chapter 3 : Energy Smart Meter Gateway Based on LoRaWAN IoT Technology. Case Study: Lebanon.

3. 1 Introduction

With the increasing demand for energy, the distribution of energy production, the integration of renewable energies and the improvements made in the IoT networks that target Building Management Systems (BMS) and power outage management, the direction was to migrate the traditional grid to be smarter and more efficient. The smart grid is the integration of IoT networking technologies within the conventional power grid[1]. IoT networks introduce smart meters that allow real-time management and monitoring of different parameters including the user's energy consumption. Building a smart grid requires the introduction and integration of a variety of smart technologies, including smart meters, smart sensors and various communication protocols. As a result, global smart grid technology consists of groups of individual technologies that cover the whole grid, from generation to transmission and distribution[2]. In developed countries, smart grids play a vital role in the deployment of the electrical system by enabling the deployment of inexpensive solutions and more powerful performance. [3, 4]. With a smart grid the small electrical systems that are not connected to the central system and deployed as a cost-effective solution for the electrification of the rural area, can then be connected to the national central power grid in a simple and easy way.

The technology of the Internet of Things (IoT) is to connect any real object to the Internet. Every object is unique recognized and accessible by the network. Last mile IoT connectivity relies on a variety of communication technologies and protocols, with the majority categorized as short-range networks that operate in ISM bands such as Zigbee, Wi-Fi, and Bluetooth. Short-range technologies have been successfully tested and implemented in various industry sectors. However, in the energy sectors, deployment is difficult in some hard-to-reach areas where reliable last-mile connectivity is necessary, between the Home Area Network (HAN) smart meters and the Meter Data Management System (MDMS). Consequently, the recent implementation of the Low Power Wide Area Network (LPWAN) technology, which provides long-range connectivity, has become a promising alternative to IoT in energy applications. Within LPWAN, a variety of technology implementations exist and operate in licensed and unlicensed spectrum, respectively such as NB-IoT, LoRaWAN, and Sigfox.

In Lebanon, the first practical experience of IoT technology in a pilot project has been demonstrated in agriculture by some private companies, where LoRa sensors were used to monitor soil moisture[5]. Concerning the energy sector, the Electricity of Lebanon corporation (Electricté du Liban, EDL) uses conventional energy meters based on electromechanical sensors, and energy consumption measurements are taken monthly by the EDL employees. Up to now, in the utility sector, the deployment of smart IoT measurement technologies depends on different requirements, such as the geographical nature of the country, consumers' attitudes towards access to their consumption data, the cost of a new intelligent meter and the cost of replacing the existing system, and a lack of adoption of appropriate standards and technologies to be used for end-to-end connectivity [6].

After a detailed presentation of the German SMGW architecture as well as the presentation of the various communication technologies that are used in AMI in the previous chapter, in this chapter, we aim to integrate the new IoT technology with the existing traditional energy meters set up in developing countries such as Lebanon, by developing an energy gateway similar to that adopted in Germany in the Lebanese case, in order to accelerate the communication between the meter and the utility in near real-time, including the AMR (Automated Meter Reading) infrastructure and giving consumers a real-time feedback on their energy consumption. So we expect that our proposed solution will illustrate the smart meter functionalities by operating independently and transmitting data to the utility using LoRa technology as last-mile connectivity on a near real-time basis. The challenge that exists in such a configuration with the current Lebanese energy infrastructure is the variety of energy providers. The Lebanese energy market relies on both diesel generators and utility[7] so the setup should be able to take both energy measurements and to transmit it to two different providers, in addition to the integration of such system with the existing traditional meters. Hence we have tried to develop a low power, long-range connectivity and low-cost gateway solution, therefore, the focus was on using LPWAN technology[8] which has recently been widley used for smart metering solutions while keeping current metering protocols intact. LPWAN technologies allow the utility to read the metering data over a longer range than conventional solutions in an urban area as we have proved in our smart energy metering prototype. Furthermore, this chapter is a Proof-of-Concept (PoC), of an open-source and low-cost technology enablement of energy smart metering architecture based on LoRa with the use of a Microcontroller (MCU) PLATFORM (Arduino MeGa 25600). LoRa is the physical layer of the LPWAN technology and operates within Unlicensed ISM bands (868 MHz in Europe, 915 MHz in North America, and 433 MHz in Asia). It is a low-cost technology that can be used to interconnect energy meters and send the energy consumption data to the cloud via a gateway. It provides a bidirectional wireless communication that is essential to implementing the metering infrastructure (AMR) in a Smart Grid. This chapter begins with a comprehensive overview of the metering protocols and the LoRa wireless technology, then the methodology of the suggested prototype subsystem in addition to the deployment procedure and experimental results are described and analyzed in the remaining sections.

3. 2 Theory

With the latest improvements in IoT networks, utilities worldwide are installing smart meters with different communication technologies. Recently, LPWAN technologies have been significantly used and deployed in today's scenarios as a long-range solution for smart metering. Usually, with a smart module that is integrated into the energy meter, the majority of smart meter functionality is achieved. Data transmission uses low-power, long-range, narrow-band transmission, leading to a more stable and reliable network with low implementation costs. This smart module could be programmed in a way to provide the utility and the consumer with notifications at predefined time intervals.

Next, we present all the knowledge about IoT that is needed to solve and give some inspiration on the methodology adopted to develop our getaway, in addition to a detailed description of LoRa and a justification for choosing LoRaWAN as our prototype communication technology.

3. 2. 1 LPWAN Technologies

LPWAN technologies take place when other technologies (like Zigbee, WiFi, and Bluetooth) aren't good enough to fill all the gaps in some case studies and even fail to achieve long-range coverage and performance[9]. For M2M cellular networks, they are too expensive in terms of equipment and services and it consumes too much energy. Therefore, LPWAN technologies are perfect for deployment for nodes that need to transmit a small amount of data over a long-range while saving the battery life[45]. The best two areas for deploying LPWAN technologies are:

- LPWAN technologies are a perfect replacement for M2M cellular technology in smart cities and buildings and other applications like smart grid, smart lighting.
- In an application that requires a long battery life, like smart agriculture and water metering.

Sigfox[10] and LoRa[11] are competitors in the LPWAN space, and both of them belong to the Unlicensed ISM bands. While they differ in the business model and the technology itself, but they are too similar in terms of functionalities and both are used and implemented for IoT applications that require a low power long-range communication protocol. Sigfox, a narrowband technology implementation, can be implemented for long-range applications. It uses the BPSK (binary phase-shift keying) modulation in the uplink and Gaussian Frequency-Shift Keying (GFSK) in the downlink, it has a data rate of up to 100bps and transmits data up to 10kms in urban areas and up to 40kms in rural areas.[12]. Sigfox endpoints are inexpensive but the base station that controls and manages the network is more complicated than the corresponding element in LoRaWAN. While LoRaWAN operates at a wider band. On the other hand, Narrowband-Internet of Things (NB-IoT) is a standard developed by the Third-Generation Partnership Project (3GPP), that uses cellular telecommunication bands to connect a wide range of nodes[13]. It is used for massive M2M and IoT applications that require an extended range of transmission with a low cost and low power for long battery life. It coexists in long term evolution (LTE) or Global System for Mobile (GSM) under licensed frequency.

In the current scenario, existing Home Area Network (HAN) technologies that are well standardized and used like Wifi, Zigbee, Bluetooth, and Z-Wave, have some challenges in terms of energy consumption and connectivity coverage. They are part of the short-range wireless communication technologies. To extend their coverage limitation due to their short physical range (less than 100 m), they use mesh network topology. Hence, their main drawback is the high deployment cost to link the large number of nodes that are geographically dispersed in a large area. Furthermore, since the data is communicated via multi hops to the gateway, a large number of nodes are more loaded and congested than others, which will have an impact on their batteries' life (i.e. excessive use of energy), and therefore the network lifetime will be affected. Similar, the 2G, 3G, 4G, LTE cellular networks are developed to have a better traffic throughput, but they are not the best solution to be used for IoT applications due to battery consumption and they are proprietary to mobile operators.

On the other hand, the next-generation cellular proposal NB-IoT for the IoT application is not yet well-deployed worldwide and specifically in Lebanon, therefore this gap is being filled with LoRa technology. LoRa is developed to operate with IoT nodes which require a long battery life and low data transmission over a long distance.

Furthermore, both short-range and cellular technologies are expensive solutions to deploy in a large area while LoRa is much simpler and presents a low-cost solution that is based on open standards.

LoRaWAN platforms are built as required and are inexpensive. LoRaWAN meets the essential requirements of IoT such as secure bidirectional communication, monitoring services and mobility. Furthermore, LoRaWAN specs afford transparent interoperability between smart things without a sophisticated implementation and provide the end-user, the developer, and the business with the right to enable the new rollout and solution with IoT.

3. 2. 2 LoRa Technology

LoRa is a powerful modulation technique for long-range wireless communication technology, low data rate, and long battery life (up to 10 years). It is patented by Semtech, and uses a chirped spread spectrum modulation for layer one or the physical layer for LoRaWAN (LoRa is the physical layer technology). The chirped spread spectrum modulation reduce the impact of interference on data transmission by providing increased reliability. LoRa MAC layer was developed by the LoRa Alliance and forms the data link and network layer. The adaptive rate is one of LoRa features, and it can be adjusted accordingly with the chosen bandwidth. The transmission energy is defined by selecting the optimum spreading factor. The LoRa transceivers that need to be integrated into the smart meter are not expensive compared to other technologies. LoRaWAN uses the ISM frequency bands at a data rate of 0.3kbps to 50kbps and transmits data within a 5 km of the urban region and 20 km of a rural area with a 243-byte payload. In Europe, the adopted frequency band is 863MHz to 870MHz, however, in the US the adopted frequency is 915Hz.

3. 2. 3 LoRa Architecture

LoRa networks are typically follow a star topology where the gateway is just a relay between the end node and the central server. The end node communicates with the gateway via LoRaWAN and the gateway communicates with the backend via the IP standard. The LoRaWAN architecture is shown in Figure 3-1.

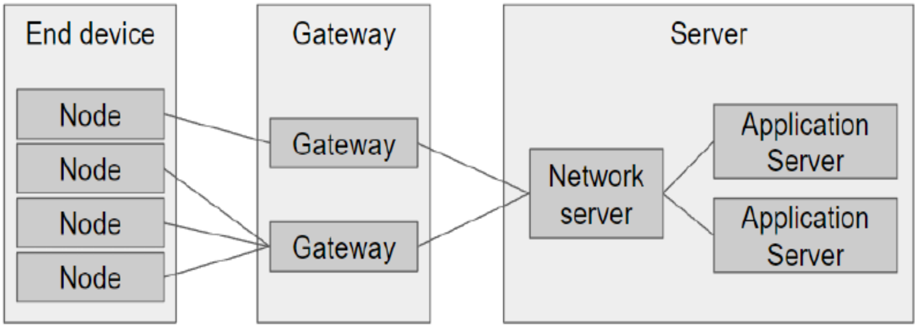


Figure 3-1: LoRaWAN Architecture

3. 2. 4 LoRa Operation Modes

LoRaWAN end devices operate in three different operating modes, namely A, B, and C, with each mode offering different uplink and downlink capabilities and energy needs accordingly[14].

- Class A nodes listen to incoming messages directly after the upload of some data and then they go back to sleep mode (batteries saving mode). The access mode used is the ALOHA mode for uplink transmission, after the transmission the class A node listens for a reply in two downlink windows, therefore, the node can be inactive for a duration of time (low duty cycle) that will save the battery life. Once the uplink transmission is successfully deciphered by the gateway then the downlink traffic can be transmitted. Hence, class A nodes are the lowest power consumption nodes with high latency in packet transmission and reception.
- Class B nodes: the gateway sends beacon messages to the end device that is used to synchronize time windows for listening. This beacon is used for additional downlink traffic without previous successful uplink transmission. Class B devices are nodes with average

power consumption and low latency in transmitting and receiving unicast and multicast packets.

- Class C devices are always in listening mode, therefore they are connected to a power supply. Class C nodes are nodes with high power consumption, with low latency in the transmission and the reception of unicast and multicast packets[15].

3. 2. 5 LoRa Evaluation Kit

LoRa Technology evaluation kit that we have used, is used in a trial validation to establish a LoRa network. The LoRa tools are developed to examine LoRa transmission and network simulation and execution. This kit contains mainly a LoRa gateway in addition to two LoRa nodes [20]. The LoRa Gateway is composed of an iC880A-SPI concentrator board, which is the base band processor and it is the Data concentrator. The gateway ensures communication with the LoRa nodes on one side and the other it provides communication with the server. Uplink messages are generated based on LoRaWAN specifications, then they are captured and transmitted by the gateway. Usually, the gateway contains 6 channels and incorporates Wi-Fi and Ethernet connectivity as well as adequate memory resources for the microprocessor that runs a Linux distribution with 16MB Flash and 64MB of RAM and is integrated with a Raspberry Pi, and Antenna.

The LoRa node contains a transceiver that is developed in accordance with LoRa technology. This module receives commands through UART interface. There are two ways to communicate with the end device the power supply, USB and battery. [21].

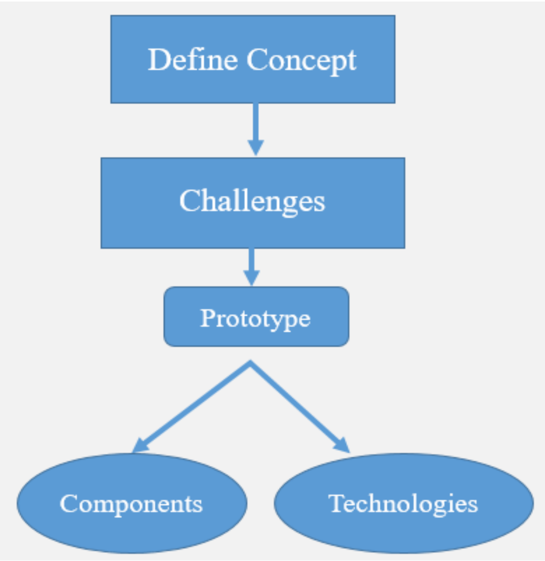
3. 2. 6 The Things Network TTN Server

The TTN is an IoT data network that utilizes the LoRaWAN technology to ensure a low power over long range wireless communication technology. It is a universal community and open sourced. It is used to link sensors and actuators to the server via transceivers. TTN give people the opportunity to develop their own end devices and connect them to gateways that are not even their own. TTN provides developers with a gateway and a network server to create their own platform.

3. 3 Methodology

The following is a description of the structure of all the work carried out to develop an energy gateway. The first is based on the definition of the challenges and problems we are trying to solve, then on the proposal of our prototype and, later on, on the definition of the components and technologies used. In a second phase once the prototype is developed, it is crucial to be implemented or simulated so that it can be tested and validated. Our final aim is to develop a low-cost open source gateway able to solve the various problems of the Lebanese energy sector. As already mentioned in the previous chapter the reference architecture and functionality will be similar to the German SMGW which is developed and used only by the German Energy Sector (exclusive for German Energy System).

The methodology adopted to develop and to verify the functionality of our system follows the below strategy presented in Figure 3-2 and Figure 3-2.



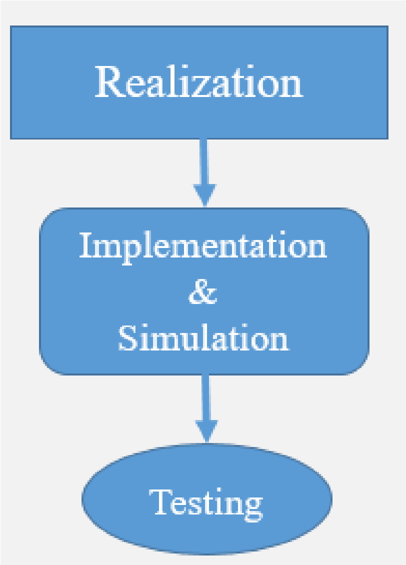


Figure 3-2: First Steps

Figure 3-3: Second Steps

3. 3. 1 Scenario Definition

The objective here is to identify a typical gateway solution where the Lebanese energy requirements are addressed. According to the existing Lebanese infrastructure scenario, an interoperable solution would have to be developed to migrate the conventional grid to a smart and intelligent grid. Therefore, it is essential to have a detailed study of the existing Lebanese scenario in order to find the right solution using IoT and LPWAN technologies. Based on the literature done, we are familiar with the German system, which is a very advanced and recent system which is the main component of the German AMI system and it is crucial to IoE enabling, in addition to the security improvements from such a system. The decision to choose our prototype component and technology is made according to existing challenges, the metering and security requirements.

3. 3. 2 Implementation and Measurement

The objective here is to implement the developed gateway and to test it in a real environment. Defining the scenario and the testing conditions means choosing some parameters to begin the simulation with and the design to be implemented. Implementation will consist of three phases:

- Metering data reading
- Metering data transmission
- Metering data visualization

Of course, the focus will be on metering data reading because of the existence of different power resources. We will use different tools to read the metering and then transmit it to an open source server.

The second objective is to take some measurements to check the functionality of the system. To make sure that the system works well and is compatible with the existing infrastructure, we had to take some serious real time measures. The measurement is to send LoRaWAN packets containing metering data and check if this data will be well received and if it is correct (which means that we have a correct reading of energy resources).

3. 3. 3 Evaluation

The main objective here is to assess the final results and extend our work to suggest future improvements. In the end, we will evaluate the system performance in terms of efficiency and correct transmission respectively to emphasize on the advantages that are presented by deploying such a system. The efficiency can be given by the number of packets lost and the delay of data transmission. In terms of security, security is ensured by the use of LoRaWAN technology which involves some security measures to avoid the eavesdropping attack and replay attacks.

3. 4 Proposed System Design and Architecture

3.4.1 Design constraints

When designing a module to convert the traditional energy meter to be smart, there are many constraints and challenges to consider and need to be predefined. The most significant challenge is the design of an interoperable module that can be easily integrated into the existing infrastructure. This design must read two different sources of energy (the Diesel and the Utility energy consumption). The following sections provide key considerations when designing such a system**.**

3. 4. 1 Design modularity and open-source

In general, modular design and open-source energy metering reading systems are for migrating traditional meters' with flexible functionality. This will ensure the reliability, scalability, and modularity of the system to fit any additional new features.

It is necessary to define some challenges and requirements before defining the hardware and software design of the system. The module designed module in this chapter is developed to add one of the smart features to the existing conventional meters. This system is user friendly and can be used by researchers to test LoRa in energy metering in the traditional gird.

3. 4. 2 Communication Protocol

For the communication network usually, a smart meter has two network interfaces: The one connected to the Home area network (HAN) where the commonly used technologies are Zigbee and Z-wave. The second network interface, the Neighbor Area Network (NAN) for communicating with the Network Operator where power line communication PLC and LPWAN technologies are used. In this chapter, we focus on the NAN area, where the designed module is developed to provide to the Network Operator, the diesel generator provider, and the consumer/end-user the ability to read the energy consumption remotely in real-time and use them in a multitude of novel ways. Establishing an NAN communication link allows the meter to communicate with other meters and the utility by using different types of existing communication protocols in our case it is LoRa. In addition, this module aims to transmit the energy consumption data via LoRa to an open-source cloud server where it can be accessed and can be operated on-premises by the different parties for energy trading applications.

3. 4. 3 Materials characteristics

Before selecting the components to be used in our module, a commercial comparison in terms of cost and performance of the existing similar components is required. The most significant technical specifications of electronic components for the performance evaluation contain accuracy, response time, and sensitivity. This applies especially to the MH-sensor-series and the Micro-Controller Unit (MCU) platform. The MCU platform should be open-source, programmed with a simple programming language based on an open-source integrated development environment, and meet requirements in terms of processing capabilities, have enough storage, and finally equipped with enough interfaces to connect to the LoRa shield and the MH-sensor. The MH sensor is an infrared sensor to detect the pulses emitted from almost any old or new smart meter that are used for the energy measurement readings.

3. 4. 4 Prototype design

3. 4. 4. 1 Hardware Design

The MH-sensor is chosen as the method of measuring the utility energy consumption. This is because it is a line detector, therefore it is able to count the number of disc rotations of the electromagnetic energy meter that is still used by the Lebanese Utility. It is a fast response sensor and it is compatible with our design. On the other hand, a relay is used to differentiate between the electricity of Lebanon EDL and the diesel generator. The Arduino Mega is used as a microcontroller unit (MCU) platform for the metering. The Arduino platform was adopted because it is open-source, user-friendly, and easy to program with a large of support from the scientific community. For data transmission LoRa shield module, which is a low-cost platform that can be easily deployed with the Arduino platform and it is used for data transmission on 868 MHz frequency between the MC and the IoT server Figure 3-4.

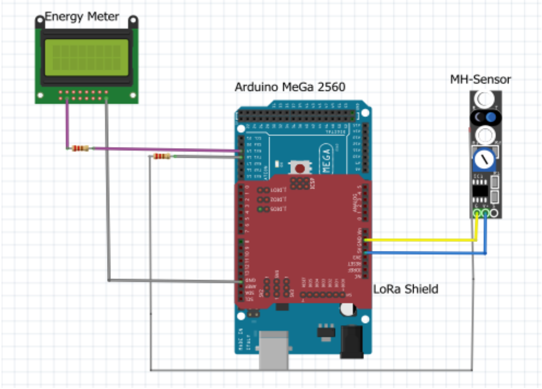


Figure 3-4: Schematic Hardware Diagram

3. 4. 4. 2 LoRa Prototype Components

In our developed system, in order to read the energy consumption of both resources, the diesel energy meter and the electricity of Lebanon (EDL) energy meter, we have integrated a LoRa module which is composed of two main components: a microcontroller connected to a LoRa shield to retrieve the energy consumption measure from the meters and transfer this data trough LoRa gateway to the network server as per the above architecture Figure 3-5. The microcontroller is the intelligent part of our entire module because it is configured to control all the components to perform and operate accordingly.

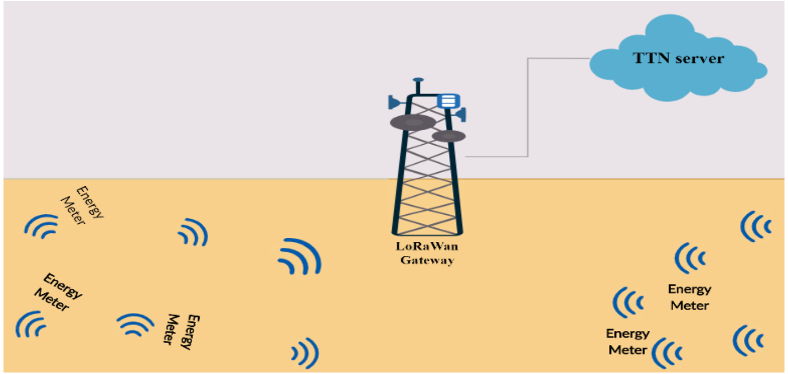


Figure 3-5: LoRa Architecture for Energy System.

In this prototype, the end device that is connected to the energy meter is composed of an Arduino MeGa microcontroller platform which integrates a LoRa shield for data transmission over a

LoRaWAN network. This implementation is represented in Figure 3-6 where the LoRa shield is interfaced with the GPIO pins on the Arduino MeGa microcontroller [16].

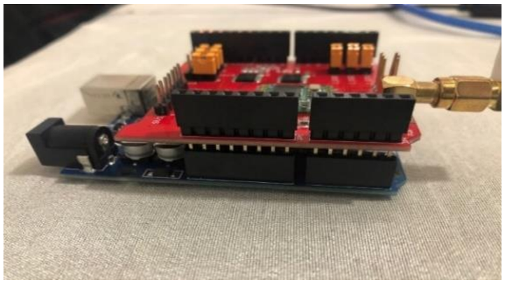


Figure 3-6: Smart meter LoRa End Node

The LoRa Gateway is composed of an iC880A-SPI concentrator board[17]. This platform integrates WiFi and Ethernet connectivity as well as sufficient memory resources for the microprocessor running a Linux distribution with 16MB Flash and 64MB of RAM and is integrated with a Raspberry Pi, an Antenna Figure 3-7.

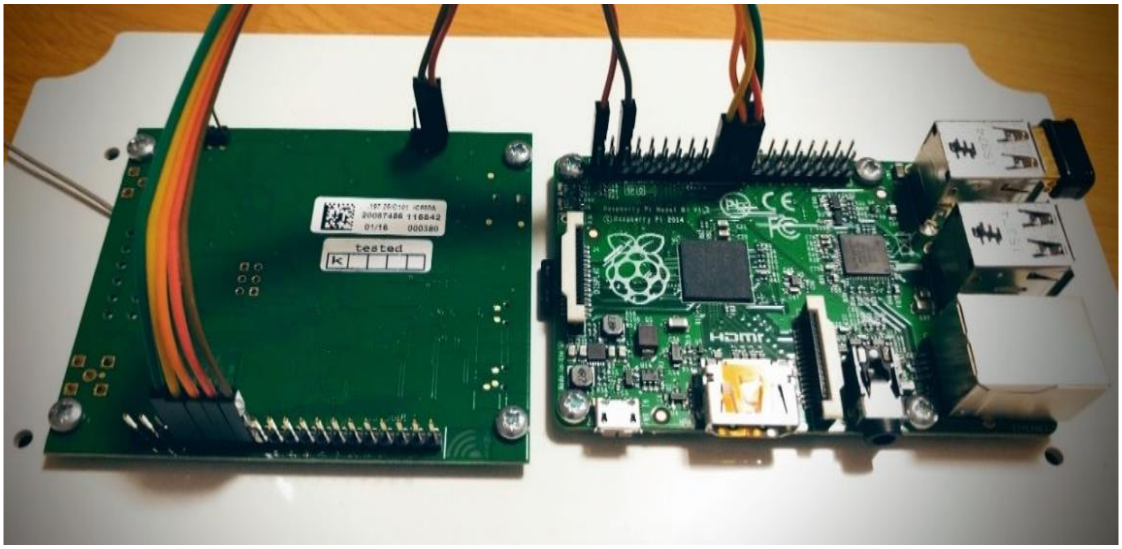


Figure 3-7: The LoRa Gateway

The LoRaWAN architecture is based on the topology star-of-stars where the gateway acts as a relay to transmit the data between the end device and the network server. The gateway is connected to the network server via the internet while the end-node is connected to the gateway via LoRa. Generally, the communication of end nodes is bi-directional, and all also support multicast communication for firmware upgrades over the air. Communication between the LoRa node and the gateway can be accomplished using a variety of frequencies and bandwidth.

3. 4. 4. 3 Connecting Nodes to a LoRaWAN Network and Data Encryption

Activation Methods:

Before joining the network and connecting to the network server, the LoRa end node must be activated through a joining procedure. This process is used to manage and control the access process and to prohibit any unrecognized or malicious end node from joining the network and participating in the communication. There are two joining methods in LoRaWAN that an end node can use:

- Activation by Personalization (ABP)
- Over-the-Air Activation (OTAA)

Over-the-Air Activation:

This activation method consists of two main commands the "Join request" and the "Join accept" that are exchanged between the end node and the network server.

Join Request

At the beginning of the joining request process, an AppKey is allocated to both the end node and the network server. The end nodes must realize their AppEUI and DevEUI, and they must be able to produce their DevNonce. AppKey is a key that is specific for the end node and it is an AES-128 root key, however the AppEUI is an application identifier, where DevEUI is a global single identifier for the end node, and finally the DevNonce it is a random number of sequences and it is produced by generating a sequence of the Received Signal Strength Indicator (RSSI) measures and it is supposed to be purely random [19].

When the activation process begins, the end node will sent a Join Request over the air, the physical payload and the format of the join request are presented in table 1 and table 2 respectively. Usually the join request message is not encrypted but in order to provide data integrity the AppKey is utilized to produce a Message Integrity Code (MIC) to provide message integrity.

MHDR	Join request or Join accept or MAC payload	MIC

Table 3-1: LoRaWAN Physical Payload Structure [19]

Join request	AppEUI	DevEUI	DevNonce
Size (bytes)	8	8	2

Table 3-2: Joining Request Format [19]

Join Accept

When the join request is sent to the network server, the server will check whether the end node is allowed to join or not usually this verification process is automatic. Moreover, the server will check the MIC, the DevEUI and the AppEUI to justify if the end node can be accepted and to which application it belongs. In case the end node is rejected the server will not reply, but if it is accepted, the server will send back the "Join Accept" message. The message format is presented in table 3.

Join accept	AppNonceI	NetID	DevAddr	DLSettings	RxDelay	CFList (Optional)
Size (bytes)	3	3	4	1	1	16

Table 3-3: Join Accept Message Format [19]

This message is composed of a 3 bytes AppNonce, which a parameter produced by the network server. AppNonce is a random number or a unique ID. The NetID is the network identifier. The DevAddr refers to the end node address assigned by the network server. However, the DLSetting, RxDelay and the CFList are utilized as physical specification. Usually the Join accept is signed and encrypted using the AppKey, while the production of the join accept message, there are two crucial session keys are produced on the network server using both the AppNonce and the DevNonce. These two keys are also produced on the end node level after receiving the join accept message. Figure 3-8 shows the OTAA activation process.

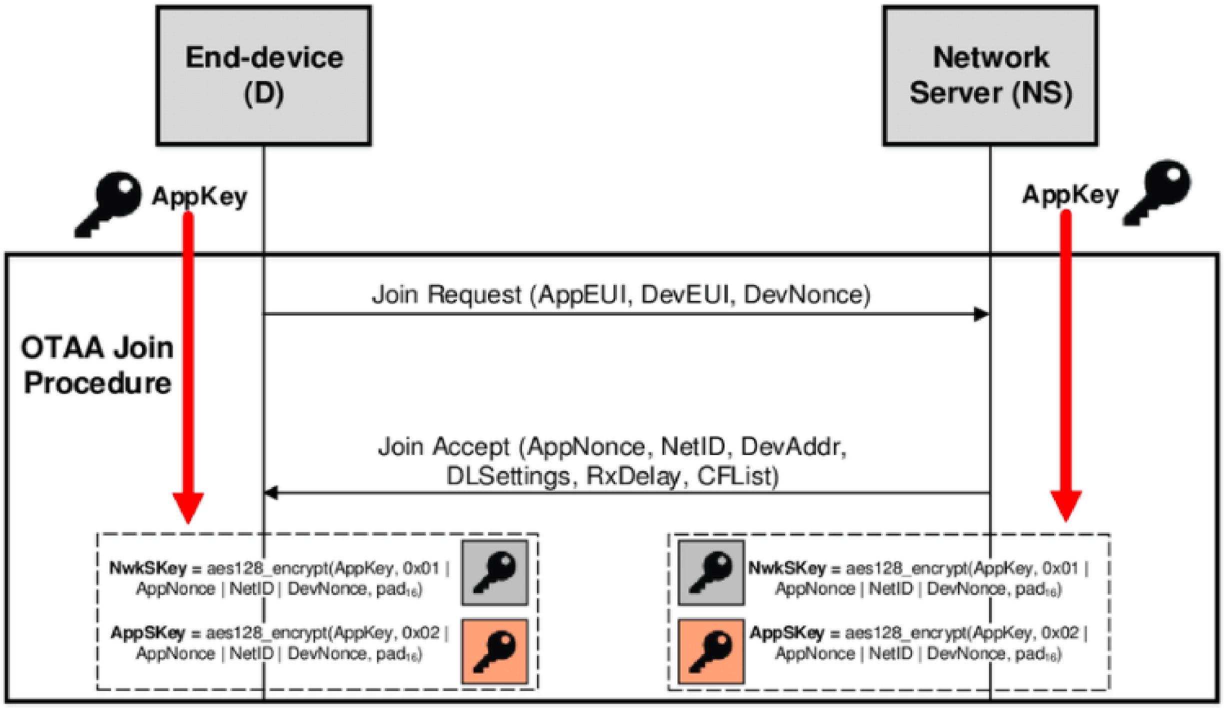

End-device (D)
Network Server (NS)
AppKey
AppKey
OTAA Join Procedure
Join Request (AppEUI, DevEUI, DevNonce)
Join Accept (AppNonce, NetID, DevAddr, DLSettings, RxDelay, CFList)
NwkSKey = aes128_encrypt(AppKey, 0x01 | AppNonce | NetID | DevNonce, pad16)
AppSKey = aes128_encrypt(AppKey, 0x02 | AppNonce | NetID | DevNonce, pad16)
NwkSKey = aes128_encrypt(AppKey, 0x01 | AppNonce | NetID | DevNonce, pad16)
AppSKey = aes128_encrypt(AppKey, 0x02 | AppNonce | NetID | DevNonce, pad16)

Figure 3-8: OTAA Activation Process [22]

In LoRaWAN network consists of 3 different types of keys: the main key AppKey and the two session Keys: NwkSKey and the AppSKey that there characteristics are presented in table 4.

Key Name	Key Type	Length in bit	Production	Utilization
AppKey	Symmetric	128	By application	MIC for Join Request and Accept Join Request Encryption Session Keys Generation
AppSkey	Symmetric	128	By AppKey	For Data Message Encryption
NwkSKey	Symmetric	128	By AppKey	MIC for messages Encrypt Command

Table 3-4: LoRaWAN Main Keys

How these tree main keys are generated?

The AppKey is a unique key per node and it is generated by the owners of the application and it is made up of 16 bytes. With OTAA the production of the AppSkey and the NwkSKey is based on the AppKey by utilizing the AppNonce and the DevNonce respectively from the network server and the end node. Each time the end node wants to reset or to join the network, the two session keys should be replicated using a new nonce. The key exchange inside the OTAA activation is presented in the Figure 3-9 below.

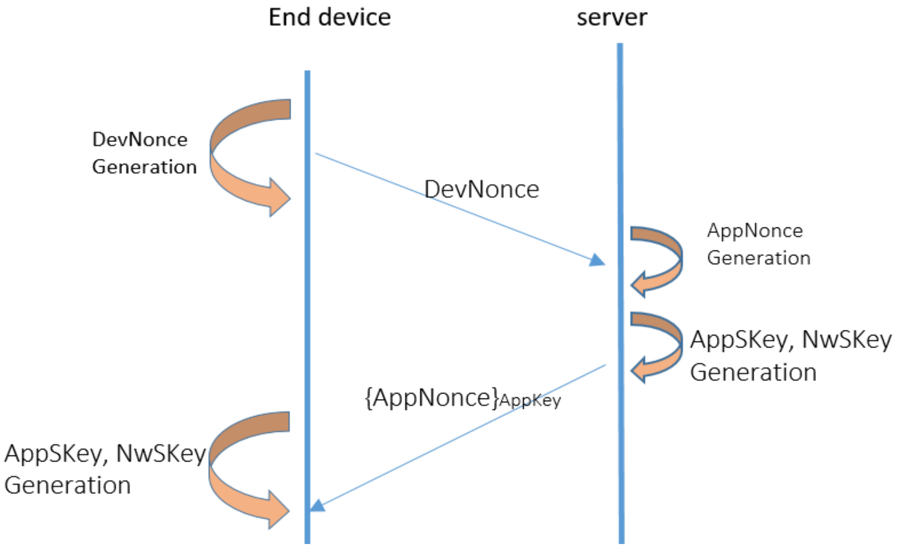


Figure 3-9: Exchange of Session Key in OTAA

Key exchange shows how keys and other data are exchanged without letting the attacker and malicious parts get a copy. The AppKey is assigned in advance before any communication, both to the server and the end node. However, for the exchange of session keys, it follows the steps in the Figure 3-9. To join the network, the end node must send a Join request to the server at the beginning and this request contains the DeNonce. If the end device is verified and is allowed to join the network, the server will return an accepted join to the accepted node, where the Join accept contain the AppNonce. Once this exchange is complete, both sides can generate the NwkSKey and the AppSKey using these two nonce.

LoRaWAN utilizes symmetric keys in an intelligent manner. Unlike the conventional symmetric key exchange, the LoRaWAN keys are not sent over the air, but the nonce are the parameters that are sent over the air. It is only when the AppKey, DevNonce and the AppNonce are all well received by both sides, the generation of the session keys is done. In this scenario, it is not easy to obtain the keys and the possibility of compromising the network has declined.

The AppKey is only utilized with the OTAA activation method, to produce both the NwSKey and AppSKey. The production process is as below:

NwkSKey = AES128_encrypt (AppKey, 0x01|AppNonce|Net ID|DevNonce|pad_16) (1)

AppSKey =AES128_encrpypt (AppKey, 0x02|AppNonce|Net ID|DevNonce|pad_16) (2)

As we can see that both session keys are produced from the AppKey and by utilizing both the DevNonce and the AppNonce.

The NwkSKey is used at the network server level (by the server operator) for encryption and decryption of command-only packets, in addition it used for signing and sign verification of information messages. AppSKey is also used at the App server level to encrypt and decrypt messages between the App server and the end node. The idea behind having 2 severs and 2 Keys is to prevent the network operator from eavesdropping application data. Figure 3-10 shows how and where the Keys are used in LoRaWAN network.

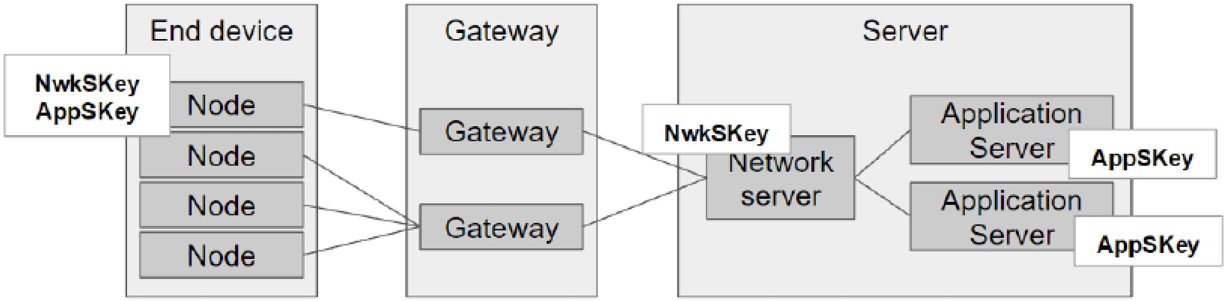


Figure 3-10: LoRaWAN Keys Utilization

The main security features of OTAA can be summarized into two points:

- Use unique settings, where Appkey, DevEUI, AppEUI, AppNonce and finally DevNonce are unique to each end node. This avoids some security breaches the whole network will not be totally compromised if an attacker was able to successfully compromise any end node.

- On the other hand, each time a new join request is received by the network server, the server is responsible for verifying the nonce and checking if it has ever been used. We call this a DevNonce buffer verification and this will prevent the occurrence of the replay attack. In case the nonce has been used, then the end node will be rejected and not allowed to access the network. And in case of the attacker is trying to copy the join message and replaying it, it is forbidden.

Activation by Personalization (ABP)

Compared to the OTAA, this activation mode doesn't have the join process, there is no exchange of Join request and accept messages. Before the activation, the DevAddr, the NwkSkey and the AppSkey, are all given, assigned and stored at the end node and are unique per node, and these keys are all also saved in the server.

So, when an end node wants to join the network will directly send an encrypted and signed message to the server, where only the server with corresponding parameter is able to read the message and decrypting it.

After a LoRa node is connected to a network, packets are encrypted using a user-supplied key[18]. The LoRaWAN uses AES128 for encryption and adds a frame counter to the packets, while the application payload is encrypted by the AppSKey and the whole packet, including the frame counter and the DevAddr, is signed by the NwkSKey. As the NwkSkey is only known from the node and the network server, the integrity of a packet can only be verified within the network where the device is registered.

3. 5 Design Implementation

3. 5. 1 Hardware Implementation

The schematic and the implemented hardware designs are represented in Figure 3-4. and Figure 3-11 respectively. As shown in Figure 3-11 the diesel generator and the MH-sensor are connected to the MC. The Arduino platform is programmed using a simple code snippet. As presented in Figure 3-6 the LoRa shield is connected to the Arduino platform. Both the LoRa shield and MH-sensor are powered by the Arduino board, while the Arduino board is supplied through a Universal Serial Bus (USB) port.

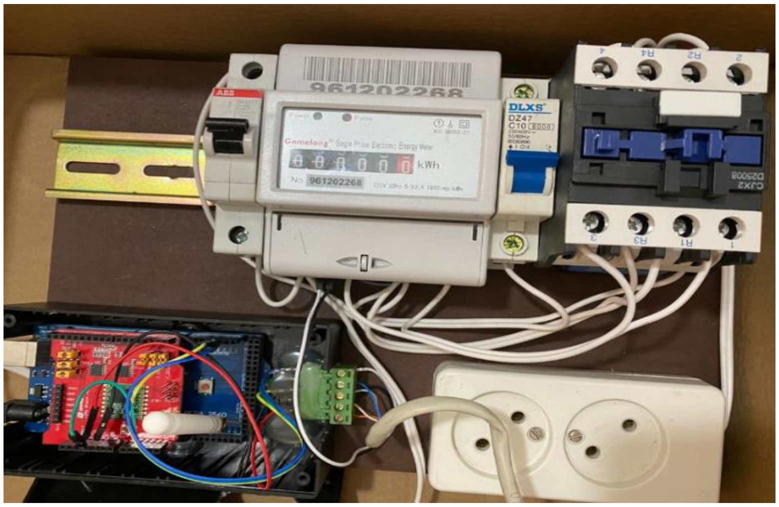


Figure 3-11: Hardware Design

In our experiment, the test is performed using the commonly used energy meters deployed on the Lebanese market, the Gomelong energy meter that is deployed by the diesel generator providers, and a line detector MH-sensor-series to read the utility's electromechanical energy meter. Both are interfaced with the microcontroller module that will transmit the data to the server network (control center) via LoRa through the gateway. The module is connected to the energy meter through an interface module and serial port connections. The Arduino MeGa 2560 is connected directly to the diesel generator energy counter and is responsible for the pulse detection and counting (1600 pulses equals to 1kW). However, on the other hand, the Arduino is connected to an infrared detector that is responsible for counting the disc rotation number of the electromechanical EDL energy consumption (300 pulses equals to 1kW). These data are then transmitted via the gateway through the internet to the TTN cloud server (open-source server) where they will be processed and used either by the generator's owner, the utility, or the consumer. The initial setup of the MC requires a baud rate of 115200 bps to be configured and Rx, Tx pins for the communications. The data is received by the MCU chip on the RX pin and is transmitted to the LoRa gateway via the LoRa shield communication interface as is depicted in the architecture proposed below in Figure 3-12.

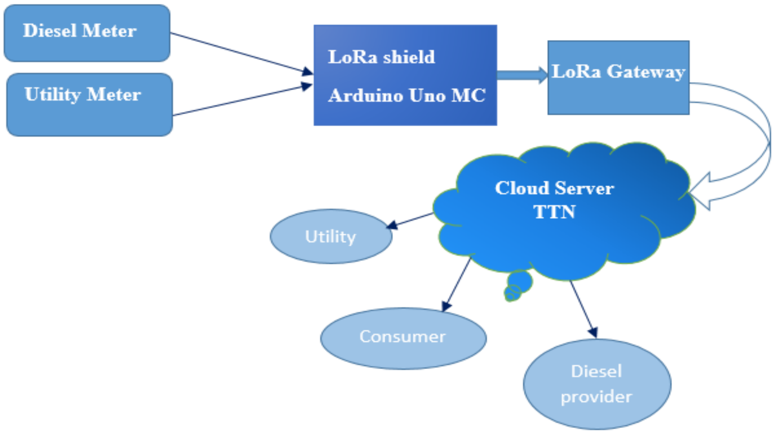
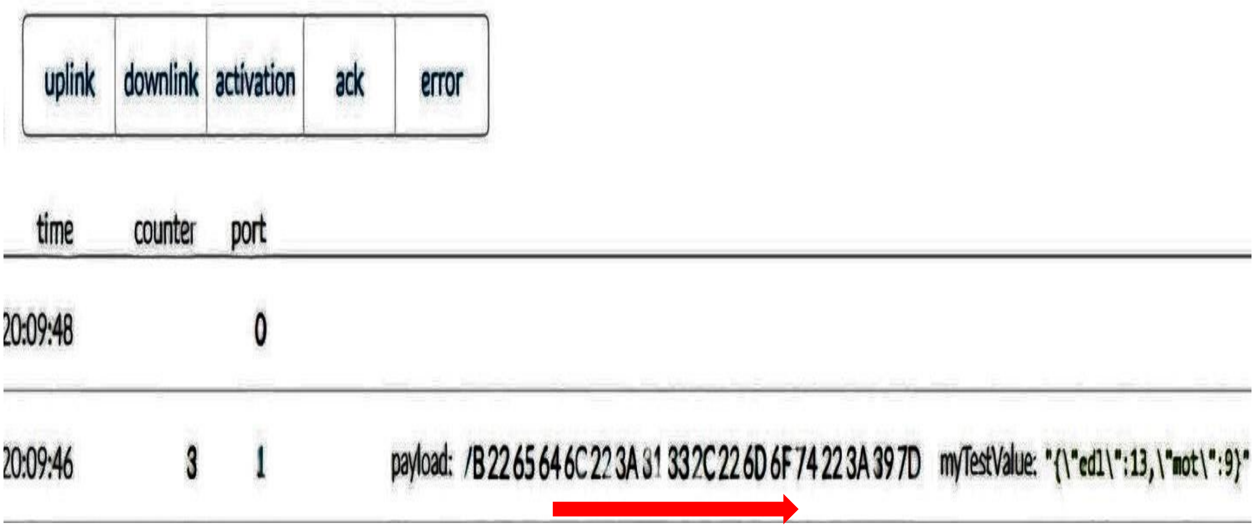


Figure 3-12: LoRa Module Connected to Energy Meters

3. 5. 2 Software Implementation

The developed code allows the MCU to count the number of pulses of each different source of energy and it sends a packet every 20ms to the TTN server. This packet consists of 2 values the EDL and the diesel generator pulse number Figure 3-13.



```
time      counter  port
20:09:48            0
20:09:46     3      1        payload: /B2265646C223A31332C226D6F74223A397D  myTestValue: "{\"ed1\":13,\"mot\":9}"
```

Figure 3-13: The TTN Server Dashboard Graphical User Interface (GUI)

3. 6 Results and Discussion

3. 6. 1 LoRa Performance Evaluation

The proposed prototype is tested with the following variables:

In the beginning, LoRaWAN performance is tested over a real environment in Beirut - Lebanon to explore the limits of communication ranges in an outdoor environment. Our experiments are based on LoRa end node and LoRa gateway and the TTN server.

The test was done under the following experimental conditions:

- Urban: Beirut City High density of users, buildings more than 4 floors
- GW Gateway, Effective Height =25m
- Antenna Height (20cm)
- The implemented code sends one packet that contains the power consumption

The transmission was tested at different distances away from the gateway. The experimental results are illustrated below:

(i) **Time on air***:* Time on air is the time to transmit a packet of data. A Spreading Factor (SF) is specified for each transmitted packet of data, the SF is equal to SF = log2 (Rc/Rs), where the chip rate is Rc and the symbol rate is Rs. As a result, there is a compromise between the communication range and SF. When the spreading factor is higher, the date rate is lower, so the communication range is longer.

The graph below shows the time on-air with a 125 kHz bandwidth channel of and a 4/5coding rate. However, as shown with a larger spreading factor, the time on-air increases.

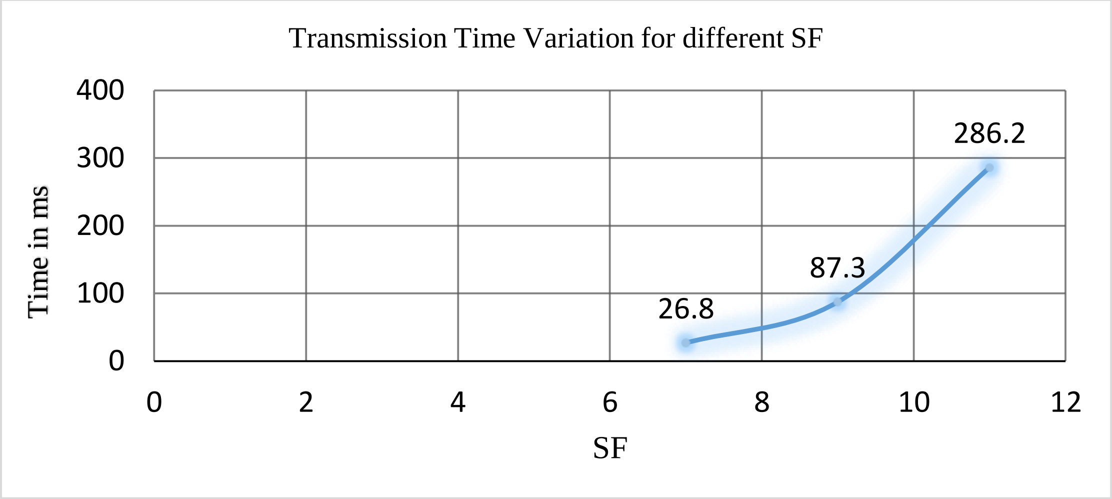


Figure 3-14: Transmission Time Variation for different SF

(ii) Signal-to-Noise Ratio (SNR): first of all, the test was done in an outdoor environment with a line of sight nearby Beirut city. Figure 3-15 shows the SNR values (in dB) at each distance with periodical packet transmission. The SNR decreases when the distance from the gateway increase.

The SNR is the ratio of the received power signal and the noise level power level. The noise level depends on all sources of undesirable interference signals that will impact the emitted signal. If the SNR value is positive, the received signal works above the noise level.

- If the SNR value is negative, the received signal works below the noise level.

Usually, the noise level is the physical limit of sensitivity, but LoRa performs under the noise level. Particularly LoRa SNR varies between: -20dB and +10dB. If the SNR rate is close to +10dB which means that the signal at the reception is less corrupted. Signals with SNR value -7.5 dB to -20 dB under the noise level can be demodulated by LoRa [15].

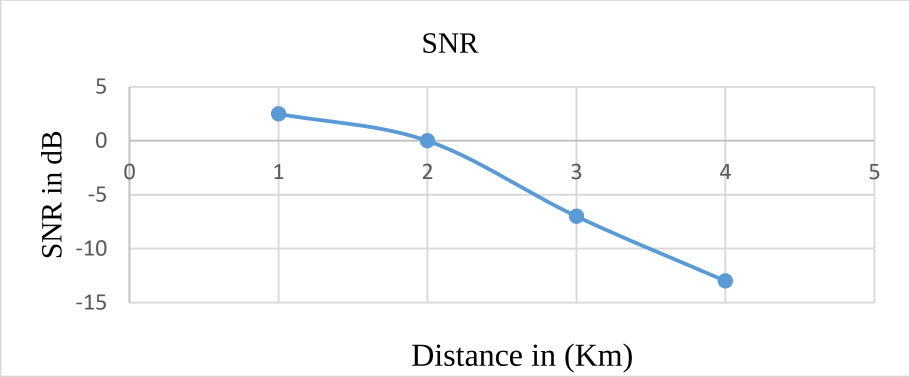


Figure 3-15: SNR Variation

Refer to the measure taken when the distance away from the gateway increases, the SNR decreases and as we can see at 3 km away from the gateway the SNR is -7dB however at 4 km it becomes -13dB.

(iii) The packet losses are about 0% at a distance of 1km and 2% at 2km. The height of the end-device plays role in the number of packet losses. Also, we can notice that the number of packet losses increases remarkably when the distance is more than 4 km according to the graph below. Therefore, the gateway cannot receive the data transmitted from the end device at a distance higher than 4 Km.

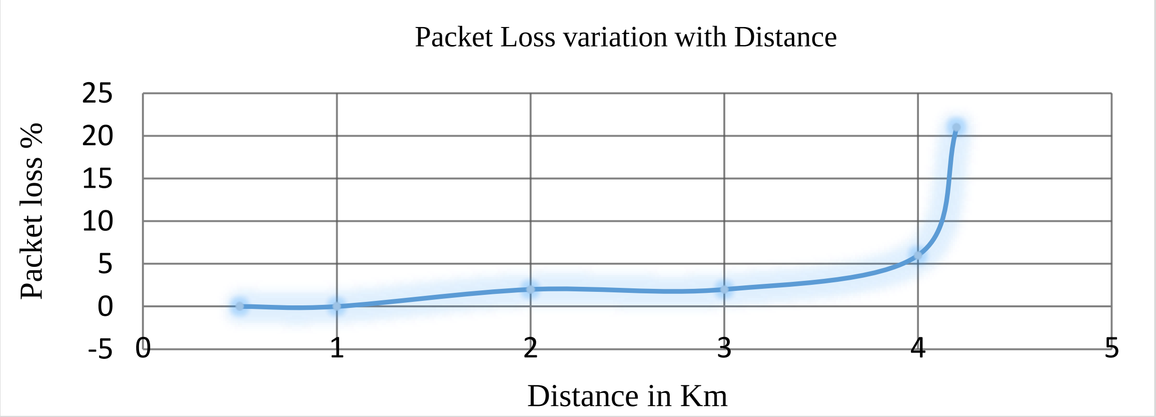
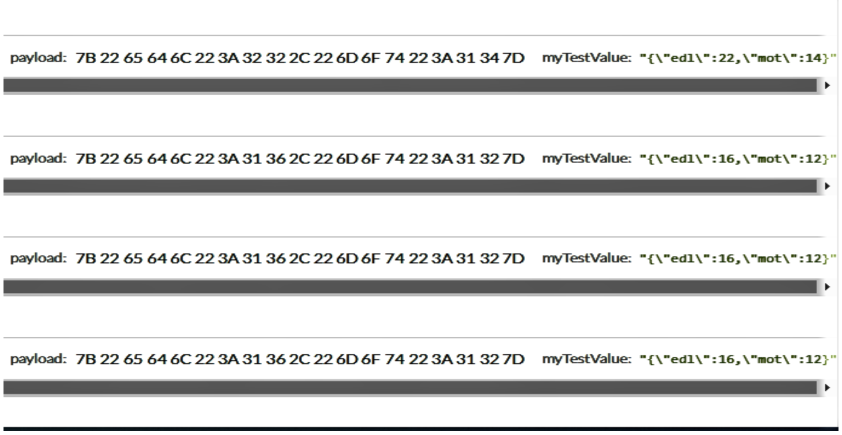


Figure 3-16: Packet Loss Variation with Distance

3. 6. 2 Results Benchmarking

The system designed for energy measurements has been tested by connecting some home appliances to create an energy load on the system. The MC and the gateway are powered on and the gateway was online and connected to the TTN cloud server. On the other hand, the MH-Sensor was connected to the electromagnetic utility meter. The responsibility of the relay is to set which power source is activated. The MC starts to count the number of pulses of the active source of energy, and then these computed measurements are communicated using the LoRaWAN and the Gateway to the TTN server by using a specific code that contains information about the different Keys to establish a secure TLS connection. The transmitted data are continuously displayed as is depicted in Figure 3-17 using the TTN dashboard GUI.



```
payload: 7B 22 65 64 6C 22 3A 32 32 2C 22 6D 6F 74 22 3A 31 34 7D   myTestValue: "{\"edl\":22,\"mot\":14}"

payload: 7B 22 65 64 6C 22 3A 31 36 2C 22 6D 6F 74 22 3A 31 32 7D   myTestValue: "{\"edl\":16,\"mot\":12}"

payload: 7B 22 65 64 6C 22 3A 31 36 2C 22 6D 6F 74 22 3A 31 32 7D   myTestValue: "{\"edl\":16,\"mot\":12}"

payload: 7B 22 65 64 6C 22 3A 31 36 2C 22 6D 6F 74 22 3A 31 32 7D   myTestValue: "{\"edl\":16,\"mot\":12}"
```

Figure 3-17: Data Display

There is a slight delay between the data packets generated by the Arduino platform serial interface and the values published on the TTN server, and this delay refers to the time taken by the LoRa shield to transmit the data packet and the cumulative delays from the TTN cloud server. This delay is not deterministic, but as it is in the order of seconds, it is considered not important by considering that the directives in the European Union for energy smart metering demand sampling periods in the order of 15 min.

To verify the setup, we have connected specific electric loads to the IoT smart meter prototype and we have verified the validity of the between the locally recorded data and the reported data using the TTN cloud server during a specific time interval.

3. 7 Conclusion

To summarize, this chapter proposes the design and deployment of an open-source, low-cost, and modular system based on LoRa telecommunication technology for energy metering applications. This solution has been designed and proposed for the Lebanese market as an important solution to access electricity outages by deploying an infrastructure for energy metering in real-time.

The design was deployed and tested in an experimental energy metering application, where the measured values were published to a cloud server, allowing analysis and accessibility from energy operators and smart meter owners simultaneously. These values can be accessed, processed, and presented using a multitude set of tools enabling the deployment of third-party valuable services like the implementation of Virtual Power Plants for Energy curtailment, the commitment of consumers to load-shifting and reduction power consumption through gamification, and the introduction of Distributed Ledger Technologies for peer-to-peer energy trading.

The proposed platform design can be easily deployed for improving the Lebanese energy sector by changing the traditional role of consumers to prosumers (producers and consumers) since most of the consumers own diesel generators and can participate in an Internet of Energy implementation.

This chapter has led to the realization of an open-source energy-smart metering solution requiring minimal intervention in an existing electrical installation with a very low budget that can be useful to the scientific community and the electricity companies for experimentation and evaluation of the implementations of IoT smart metering technology.

In the following Chapter, and in order to extend our work, we developed standards that comply with the international and European standards, the prototype will be developed to support the transmission of DLSM/COSEM protocol (which a metering protocol that is used in Europe and the United States of America). The different constraints and challenges will be identified and simulations will be launched.

Chapter 4 : Open Source LoRaWAN Telemetry Test Bench for Smart Grid – a DLMS/COSEM Implementation Case Study

4. 1 Introduction

Internet of Energy (IoE) emphasizes the need for a smart and adaptive Energy Grid system based on smart energy meters (SM) and IoT communication technologies. However, many countries remain unable to meet their SM deployment plans due to obstacles such as the lack of human and financial resources, and the absence of interoperable and globally standardized communication protocols in the energy sector. Therefore, the development of an open-source platform that can be implemented on top of the existing legacy infrastructure, while having the capability to transmit metering data using a proven, easily adaptable, and already established long-range wireless communications technology, could accelerate the anticipated migration to Smart Grids.

The purpose of this chapter is to build a low-cost open-source telemetry platform, based on the previous German SMGW (already presented in previous chapter), capable of integrating energy meters that comply with the DLMS/COSEM standards with LoRaWAN.

DLMS/COSEM is the worldwide standard application protocol for smart energy metering, control, and management that is widely accepted in Europe and the USA. In the proposed architecture, the electricity telemetry data (consumption or generation) is then transmitted to a blockchain network, through a LoRaWaN application server, to be certified and consumed by Distributed Applications (DApp). In this way, producers and consumers will be able to trade (sell or buy) energy (especially from distributed renewable energy sources) over the existing infrastructure, using blockchain technology to improve integrity, transparency, and security, leading thus to a peer-to-peer electricity trading platform and the democratization of the energy market.

With the growing energy demand, the energy generation distribution, the integration of renewables sources and grid management challenges (e.g., outage management) on one side, and the explosion of IoT networks in Building Management systems (BMS) on the other, the energy sector has been forced to shift from the transformation of the traditional grid to a smarter and more efficient grid. The smart grid is the integration of smart metering, actuation and networking technologies into the conventional electrical grid [1]. Building a Smart Grid (SG) consists of integrating a variety of smart technologies including smart meters, smart sensors (e.g., phase measurement sensors) and actuators, and different communication technologies based on standardized protocols for data exchange. As a result, the global smart grid technology is made up of groups of individual technologies that cover the whole spectrum of grid management processes, including generation, transmission, and distribution[2]. In developed countries, smart grids play an essential role in the secure operation of the electricity distribution system by enabling the deployment of low-cost solutions and more powerful performance [3, 4]. With a smart grid, small and distributed sources of renewable energy initially deployed as a disconnected and cost-effective solution for the rural electrification can then be seamlessly integrated into the national central electricity system.

The smart grid opens access to the markets through new transmission paths and demand response initiatives. On the other hand, one of the most important features of SG is the combination of secure, and reliable data communication networks to successfully manage the sophisticated power system. Thus, this complex cyber-physical power system is sensitive to problems that are related to connectivity, communication, and topology modifications.

SG standardizations are important and crucial and need to be carefully taken into account. For this, W. Wang, et al. [4] and Z. Fan, et al. [5] describe the architecture of the existing SG communication networks and they present SG's protocols and standards. The three most important standards that have been proposed to enhance and develop the SG are the Distributed network protocol (DNP), Open smart grid protocol (OSGP), and the combination of Device Language Message Specification (DLMS) with Companion Specification for Energy Metering (COSEM), a.k.a. DLMS/COSEM. The DNP emerged in 1998, the DNP3 version has been implemented in distribution substations and used for equipment control and monitoring. The main function of this protocol is to transmit the equipment status to the control station and transfer configuration commands to the equipment. But DNP3 cannot guarantee the quality of communication. The OSGP [6] suggested by the European Telecommunications Standards Institute (ETSI), is used in combination with the ISO/IEC 14908 standard for SG network controlling. OSGP protocol affords a reliable transmission of commands and control information to the smart meter (SM), the Gateways, the Renewable Energy Sources, and the intelligent power measurement and control devices within the SG. DLMS User Association (UA) provides the DLMS/COSEM which is a group of international standards for energy metering. The energy meter is considered to contain all the information such as energy consumption, registration, and maintenance[7]–[9]. COSEM combines a suite of protocol layers (Transport Layer and Application Layer) to be integrated with DLMS. Their combination, DLMS/COSEM, is adopted for energy metering data exchange as an interface model protocol for the meter functionality. This protocol has been deployed worldwide and has attracted a considerable interest from various large companies, utilities, and researchers.

This chapter begins with a description of the DLMS/COSEM protocol, where later a recall of the LPWAN communication technologies and especially LoRaWAN is given. The latter is proposed for the connection between an Advanced Metering Infrastructure (AMI) energy meter and a Data Concentrator Unit (DCU) [10], as it is increasingly adopted by utilities to support its own needs for IoT solutions. After the realization of an energy gateway that is adopted to the Lebanese case study in the previous chapter, this work aims to propose and implement an open-source, low-cost test bench to test and develop a solution allowing the use of modern technologies to evolve energy trading between prosumers and consumers, by using the standardized telemetry protocol, and that is compatible to the telemetry protocols that are used in Europe and the USA. The solution provided can read DLMS /COSEM compliant energy meters and transmit the readings to an equivalent gateway via LoRaWAN using an appropriate adaptation protocol for packet compression.

Moreover, the proposed test bench optimizes data integrity and increases security by uploading the gathered energy data onto a blockchain to achieve energy market linearization where prosumers and consumers can exchange energy via a platform connected to the blockchain network. Such a platform would help developing countries that stand unable to meet the SM rollout projects and convert their conventional grid to a smart one due to the complexity induced by a missing interoperable and globally standardized communication protocol.

The equipment used was chosen to be inexpensive and versatile, making it possible to implement and study on a large scale energy exchange scenario with the existing infrastructure, including in the current case, the constraints of implementing DLMS/COSEM over LoRaWAN. The rest of this chapter gives an overview of the SG system, provides technical details about the DLMS/COSEM protocol, discusses the metering protocols and the LoRaWAN wireless technology and finally the proposed prototype is presented, in terms of setup, deployment procedure and at the end the experimental results are explained and analyzed.

4. 2 Theory

4. 2. 1 Smart Grid and Advanced Metering Infrastructure

A Smart Grid is the new generation of the conventional electricity infrastructure that is will be a solution for improving the electrical energy system not only by integrating Renewable Energy Resources (RES), but also the Distributed Generation (DG) and Distributed Storage (DS). Smart Grid targets to solve different existing problems in power supply, respond to climate change, improve energy efficiency and localization of energy exchanges opening up a new direction in electricity markets (like Peer-to-Peer P2P energy trading). A direct implication of the Smart Grid is to have an electrical model that is able to handle different generation and storage devices in an efficient and decentralized way by deploying an Advanced Metering Infrastructure (AMI) where Smart Meters (SM) are the main components. A SM provides an accurate and remote measurement reading and communicates with smart appliances to effectively manage their energy consumption. These features are made possible by two-way communication and advanced sensors. To achieve the two-way communication, AMI architecture uses different communication networks, each one having its requirements and considerations [11]: Home Area Network (HAN) for energy management at the consumer end, Neighborhood Area Network (NAN) as the last mile for providing the AMI and Wide Area Network (WAN) realizing the communication between all pieces of the SG including control center, renewable energy sources, and transmission, and distribution of Electricity. The HAN is connected to the WAN via NAN. The NAN provides the networking infrastructure for SMs and the data collected will be transmitted to the DCU (Data Concentrator Unit), which acts as a gateway between the SMs and the electricity substations. A high transmission data rate is required at the WAN level, and therefore, different wireless communications technologies than the ones used at the HAN/NAN level, e.g. WiMAX, 3G/LTE, and micro-wave are among the proposed ones [12]. Each type of network has specific needs in terms of data rate. Table 1 shows the various communication technologies and required data rates that may be used at each level of the network hierarchy.

Network Type	Transmission Range	Required Data Rate	Possible Technologies
HAN/BAN	10 (m) - 100 (m)	Applications are using low data rate devices for communication	Zigbee, Wi-Fi, PLC
NAN	100 (m) - 10 (Km)	Depends on node density in the network	Zigbee, Wi-Fi, LoRaWAN, Sigfox, Cellular, NB-IoT
WAN	< 10 (Km)	High-end devices (routers/switches) with high speed (100Mbps)	Fiber optic, 3G/4G/ LTE WiMAX, NB-IoT

Table 4-1: Required data rate and potential communication technologies based on the Network Type

4. 2. 2 The DLMS/COSEM Standard

Here, we present a basic review of the DLMS/COSEM and data packet format to provide a foundation for the work that will presenter later in this chapter.

The DLMS/COSEM is an interface model that is developed and used to share energy meter data and information. This interface model gives a view of the meter functionality as it is available at its interfaces. However, communication protocols specify how data can be accessed and transmitted. DLMS UA standard is described and presented in four documents: Green Book, Yellow Book, Blue Book, and White Book [7]–[9]. The blue book presents COSEM meter object model and the object identification system (OBIS). The architecture and protocols are described in the green book.

The DLMS and OSI communication profiles are presented in Figure 4-1. These communication profiles can be grouped into two parts with the Application Layer first and all other layers secondly. The application layer is composed of three layers: the COSEM Application Process layer, the COSEM Application Layer, and finally the COSEM connection manager layer. The lower layers are divided into three different ways based on the type of communication.

These three different categories include CO-HDLC which is directly the data link and the physical layer and does not have a transport layer. The data link layer contains two sub-layers the LLD and the HDLC. However, TCP-UDP/IP communication type contains a transport layer, where on top of it a wrapper sub-layer is added, and a data link layer. Finally, IEC61334-5 S-FSK PLC profile is proposed for PLC communication that includes the data link and physical link layers Figure 4-1.

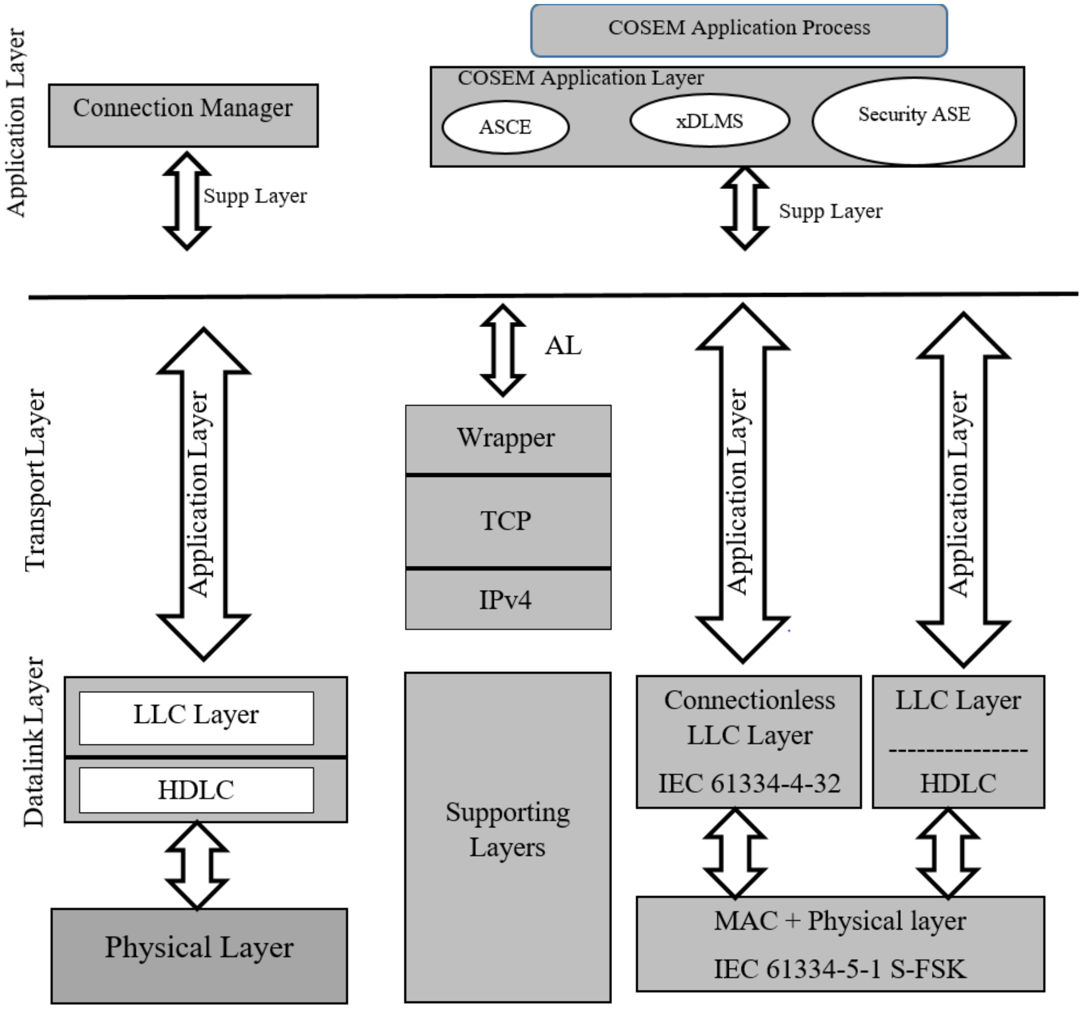


Figure 4-1: DLMS/COSEM Communication Profiles

DLMS/COSEM sequence the data exchange between the energy smart meter and the DCU and is based on the client-server model, where the client will be the DCU and the energy smart meter serve as a server. For DLMS/COSEM the establishment of a connection between DCU and the SM is based on a packet exchange sequence of, which is divided into three phases: data link setup, data transfer, and finally the data link disconnection shown in Figure 4-2.

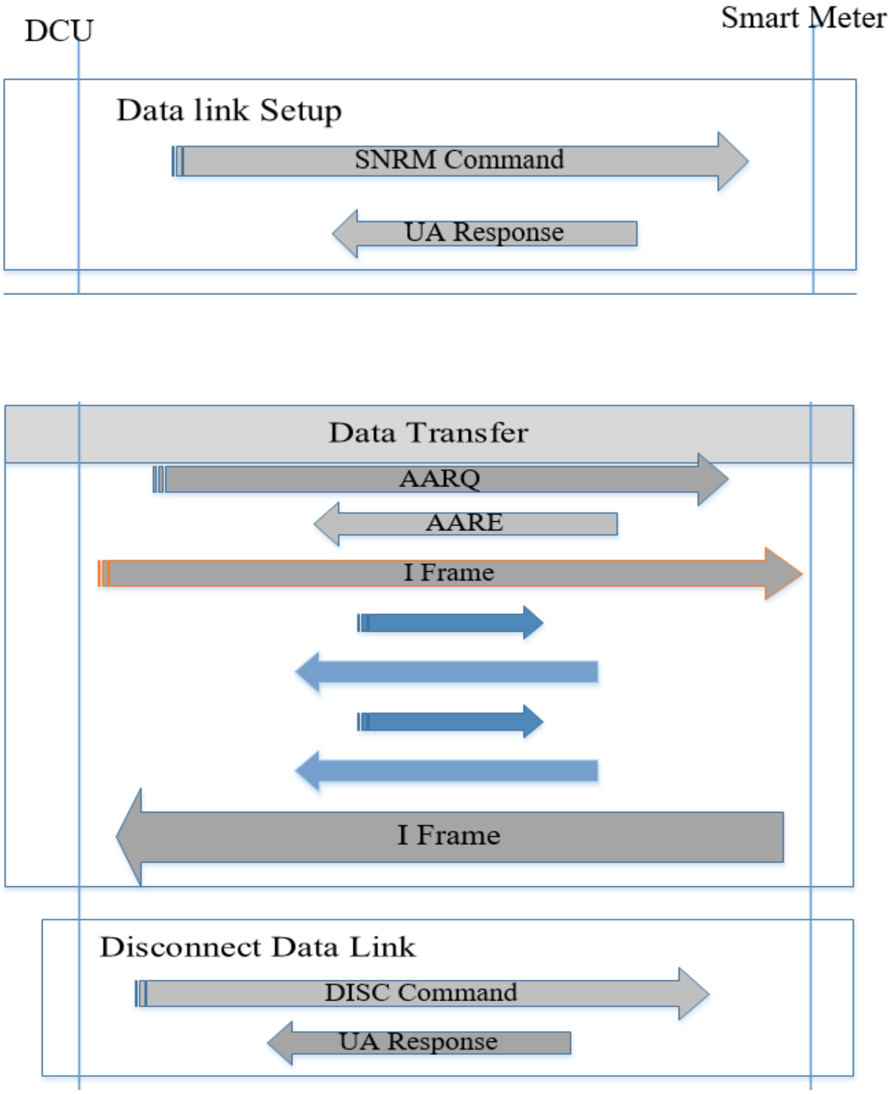


Figure 4-2: Connection Establishment and Packet Transfer of DLMS/COSEM

In the data link setup sequence, the DCU initiates a Set Normal Response Mode (SNRM) command to the SM. At the reception, if the SM is ready to establish a connection, it will send back an acknowledgment response named Unnumbered Acknowledge (UA).

In the data transfer sequence, once the DCU receives the UA and before establishing a connection, it initiates a command to check the SM properties called A-Associate Request

(AARQ). In its turn, the SM will reply by sending the A-Associate Response (AARE). The AARQ packet contains all properties that a meter can have and the AARE is the meter properties. Once these packets exchange is completed now the DCU and the meter can exchange I-Frame (information packet).

In the data link disconnection sequence, when the data exchange between the DCU and the SM has been completed the DCU sends a disconnection command (Disconnect DISC) and the SM sends a UA response for confirmation.

DLMS/COSEM Packet Exchange Sample

The COSEM application process contains the Interface Class and Object Identification System code (OBIS). There is a class identity (class_id) for each interface and the number of interfaces depends on the type of process (e.g., for the data storage process there are nine interface classes as presented in Figure 4-3. OBIS code is a code for an identified parameter that DCU used to ask from SM. OBIS code is composed of six (6) groups from A to F where:

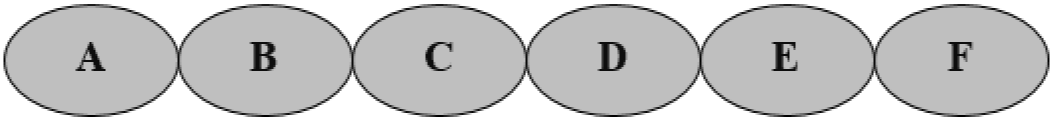


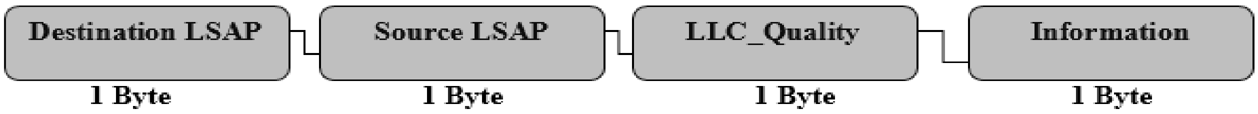
Figure 4-3: OBIS Structure

- Group A includes the data that we want to measure like gas electricity usage.
- Group B defines the type of channel in use like HDLC, RS232, and TCP-UDP/IP.
- Group C defines the parameter of the data source, including voltage, power, and temperature.
- Group D defines the measuring process of physical quantities that are related to the parameter of group A.
- Group E defines other measuring information like electricity fees.
- Group F defines historical information within the meter concerning group A to E parameters.

The COSEM application layer is divided into three sections: ACSE, xDLMS, and Security ASE (application service element). The xDLMS is a connection-oriented application protocol that is simple and easy to be read and understand by a human. The COSEM application layer will transform the xDLMS code to an Application Layer Protocol Data Unit (APDU). The size of the APDU is dependent on the length of the xDLMS and Table 4-2 represents the APDU size of the exchange commands and responses between the DCU and the SM to establish a connection. The APDU will be transmitted to the lower layer by the COSEM application. In this study, only the transmission over CO-HDLC is considered. In our case, the data link is composed of two sub-layers the LLD and HDLC. The frame format of each sub-layer is shown in Figure 4-4 and Figure 4-5 respectively. After the data link, the frame will be transferred to LoRaWAN's physical layer (PHY).

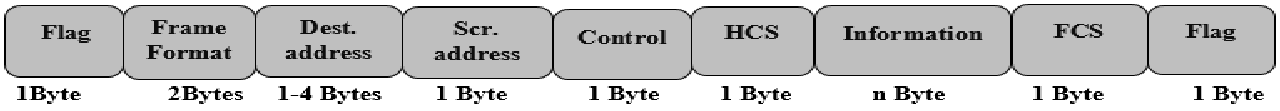
Packet type	Frame	Size in (Byte)
SNRM	7EA00000020023219318717E	12
UA	7EA023210002002373F6C581801405020080060 20080070400000001080400000001CE6A7E	33
AARQ	7EA02E0002002321107ECBE6E600601DA1090 60760857405080101BE10040E01000000065F1F 040000301DFFFFD4C57E	48
AARE	7EA03A2100020023309941E6E7006129A10906 0760857405080101A203020100A305A10302010 0BE10040E0800065F1F040000301D190000070 C527EE	60

Table 4-2: Commands APDU size in bytes



Destination LSAP	Source LSAP	LLC_Quality	Information
1 Byte	1 Byte	1 Byte	1 Byte

Figure 4-4: LLD Frame



Flag	Frame Format	Dest. address	Scr. address	Control	HCS	Information	FCS	Flag
1Byte	2Bytes	1-4 Bytes	1 Byte	1 Byte	1 Byte	n Byte	1 Byte	1 Byte

Figure 4-5: HDLC Frame

4. 2. 3 LPWAN Communication Technologies and LoRaWAN Recap

With the latest improvements in IoT networks, global utilities are installing smart meters with different communication technologies. LPWAN technologies can be widely used and deployed in today's scenarios as a long-range solution for smart metering. With a smart module that is integrated into the energy meter, most of the functions of the smart meter can be achieved. Data transmission uses low power, long-range, and narrowband transmission features which lead to a stable and reliable network in addition to the low-cost benefits of the implementation. This smart module can be programmed so as to provide the utility and the consumer with notifications at predefined intervals of time.

LPWAN technologies take place when other technologies (like Zigbee, Wi-Fi, and Bluetooth) are not good enough to fill all the gaps in some case studies and even fail to achieve long-range coverage and performance [13]. M2M Cellular networks on the other side, are too expensive in terms of hardware and services and their nodes increased the demands for energy consumption to be autonomous. Hence LPWAN technologies are ideal to be deployed for nodes that need to transmit a small amount of data over a long-range while saving battery life [14]. The best two areas for deploying LPWAN technologies are:

- Smart cities and buildings, where LPWAN technologies are a perfect replacement for cellular M2M ones, for applications such as smart grid and smart lighting.

- Application domains where communication needs include low bandwidth but long battery life for the autonomous nodes (e.g., smart agriculture and water metering).

LoRa is a strong modulation technique for long-range, low data rate, and long battery life (up to 10 years) wireless communication technology. It is patented from Semtech and uses a chirped spread spectrum modulation for layer one (the physical layer) for LoRaWAN. Chirped spread spectrum modulation reduces the impact of interference on data transmission by providing increased reliability. LoRa MAC layer was developed by the LoRa Alliance and forms the data link and network layer. Adaptive rate is one of the LoRa features, and it can be adjusted accordingly with the chosen bandwidth. The transmission energy is defined with the selection of the optimum spreading factor. The LoRa transceivers that must be integrated with the smart meter are not expensive compared to other technologies. LoRaWAN uses the ISM frequency bands at a data rate of 0.3kbps to 50kbps and transmits data within a 5 km range in the urban area and 20 km in a rural area with a 243 bytes payload size. In Europe, the adopted frequency band is 863MHz to 870MHz, however, in the US the adopted frequency is 915Hz.

LoRa networks generally follow a star topology where the gateway acts as a relay between the end node and the central server. The end node communicates with the gateway via LoRaWAN and the gateway communicates with the backend via the IP standard. LoRaWAN end devices operate in three different operation modes, namely A, B, and C, with each mode offering different uplink and downlink capabilities and energy needs accordingly [13].

- Class A nodes listen to incoming messages directly after the upload of some data and then they go back to sleep mode (battery saving mode). The access mode used is the ALOHA mode for uplink transmission, after the transmission the class A node listens for a reply in two downlink windows, therefore, the node can be inactive for a period of time (low duty cycle) and therefore increase the battery life. Once the uplink transmission is deciphered successfully by the gateway then the downlink traffic can be transmitted. Hence, class A nodes are the lowest power consumption nodes with high latency in the transmission and the reception of packets.

- Class B nodes follow a different policy: the gateway sends beacon messages to the end device which is used to synchronize time windows for listening. This beacon is used for additional downlink traffic without previous successful uplink transmission. Class B devices are nodes with average power consumption and low latency in transmitting and receiving unicast and multicast packets. In our case, we have based the experimental setups on Class B end nodes as they provide mandatory bi-directional communication for DLMS/COSEM, and also supports multicast communication for firmware upgrades over the air.
- Class C devices are always in listening mode; therefore, they are connected to a power supply. Class C nodes are nodes with high power consumption, with low latency in the transmission and the reception of unicast and multicast packets [15].

In the actual scenario, the existing Home Area Network (HAN) technologies that are well standardized and used such as Wi-Fi, Zigbee, Bluetooth, and Z-Wave, face some challenges in terms of power consumption and especially connectivity coverage. They belong to the short-range wireless communication technologies. To expand their coverage limitation due to their physical short-range (less than 100m), they commonly use a mesh networking topology. Hence, their major drawback is the high cost of deployment cost to link a substantial number of nodes that are geographically scattered in a large area. Furthermore, since the data is communicated via multi hops to the gateway, a considerable number of nodes are more loaded and congested than others which will have an impact on the life of their batteries (i.e., excessive use of energy), and therefore the network lifetime will be affected. Similar, the 2G, 3G, 4G, LTE cellular networks are developed to have a better traffic throughput, but they are not the best solution to be used for IoT applications due to battery consumption and they are proprietary to mobile operators.

Both short-range and cellular technologies are expensive solutions to deploy in a vast area while LoRa is much simpler and presents a low-cost solution that is based on open standards. Furthermore, the proposed next-generation NB-IoT cellular services for the IoT application is not yet well-deployed around the world, leaving a gap that is filled by LoRa technology, effectively servicing IoT nodes requiring a long battery life and low data transmission over a long distances.

LoRaWAN platforms are built by design according to these requirements and they are low-cost platforms. LoRaWAN meets the essential IoT requirements for transparent interoperability between smart objects, without a sophisticated implementation. They provide the IoT ecosystem with secure bi-directional communication, tracking services, and mobility, this facilitates the rollout of new solutions or the smooth expansion of the existing solutions.

4. 2. 4 Blockchain Enabling Technology for Energy Trading and Data Integrity

Global electricity networks were first built for unidirectional power flow, with fiat money flowing in reverse (Fiat money is an established currency as money, often through government regulation.). Producers were expected to be larger than consumers, but as the potential growth of prosumers has changed due to advance in technology advancements, a lot of challenges are currently under consideration. Reconstructing power networks is a difficult challenge to tackle, but re-engineering the electricity market is a different one.

Blockchains, in general, provides a distributed network, ensuring information replication and operational resilience, and stability by leveraging a distributed infrastructure, while reducing the costs of installation and maintenance of centralized resources. This is done by distributing computational and storage requirements among all the blockchain nodes that make up the network. This allows participants who may not be familiar with each other to conduct business directly and securely. The medium for this is Smart Contracts, which implement the necessary rules and actions that need to be carried out for any related business transaction, automatically and securely. Thus, such an approach eliminates the need for intermediaries, control or certification authorities like legal representatives, banks, brokers, or even the government to intercede and supervise transactions between two or more parties.

Blockchain will most probably disrupt the energy sector, in the following individual areas [17, 19]:

- Finance enhancement of distributed energy sources and battery storage.
- A solution to the split-incentive problem with multi-owner properties.
- Optimized utilization and increased value of network assets.
- Affordable and easier access to modern energy markets even for entry-level prosumers.
- Enablement of a decentralized platform for generating and distributing power.

According to [19] there are seven different research domains regarding blockchain and energy:

1. The decentralized energy markets
2. Micro grid and Smart grid
3. Energy internet
4. Smart contract
5. Peer-to-peer (P2P)
6. Renewable energy
7. Electric vehicle

In our case, we combine the DLMS/COSEM interface model and communication protocols to exchange data with smart meters and then upload them to a blockchain network. Generating, signing, and sending transactions from constrained resource devices is a task that needs sophisticated engineering. As in the case of our scenarios were not only the microcontroller-based communication module needs to be plugged in the smart meters, but also to support a wide variety of meters and standards according to the SM manufacturer and the country under deployment. For this, the connection to the blockchain network has to be done on the server-side.

After certifying the data immunity by registering them on the blockchain network, then any device capable of running cryptography algorithms can directly utilize the benefits of smart contracts. Therefore, in an end-to-end adaptation of the COSEM protocol's services, we suggest their implementation in the corresponding smart contracts.

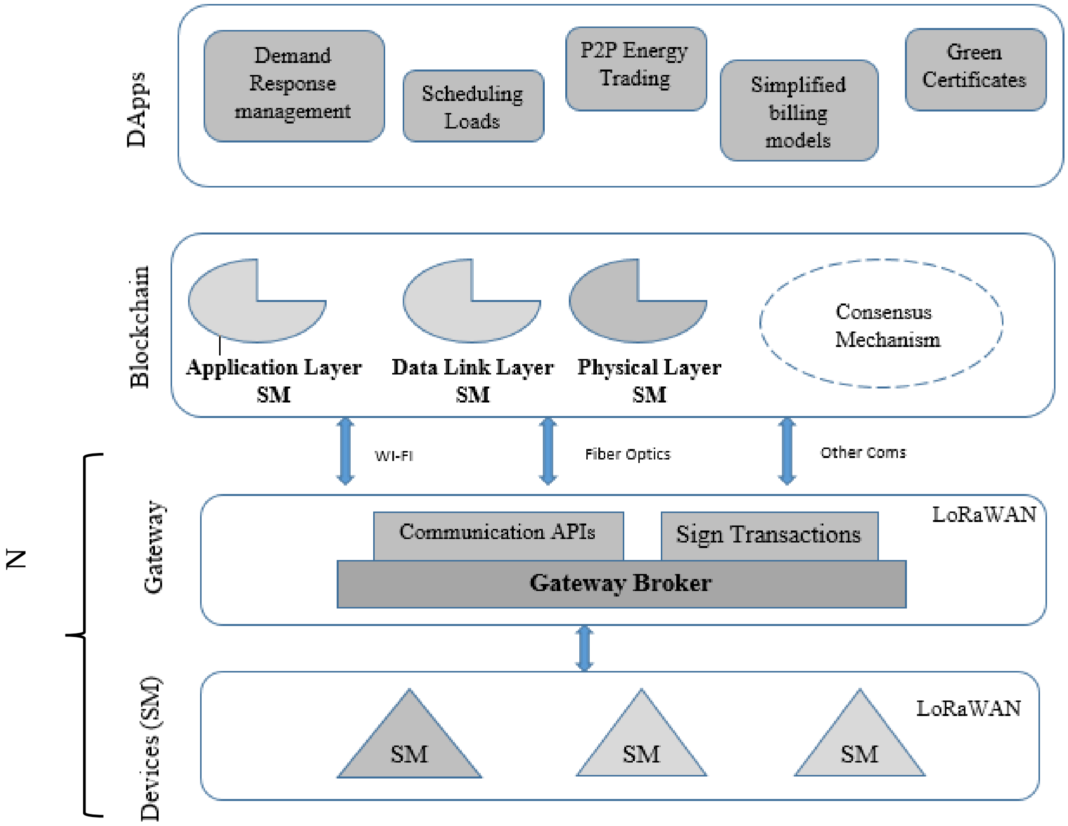


Figure 4-6: Proposed Architecture for Smart Meters Integration to a blockchain-based P2P electricity trading platform

In Figure 4-6 the proposed system architecture is visualized in four hierarchical layers which are summarized as follows:

- Devices are the Smart Meters with the appropriate hardware and firmware that enables the data transmission of measurements over LoRa and control over other conventional communication technologies such as Zigbee, Wi-Fi, etc.
- Gateway is the device(s) that gets these measurements and signs them as transactions to forward them to the Blockchain layer. In this layer, the control commands for Smart Meters are also forwarded from the corresponding Smart Contract outputs.
- At the Blockchain layer, several Smart Contracts is deployed along with the Consensus Mechanism responsible for the validity of the information

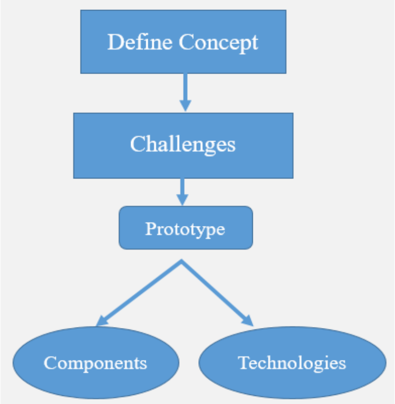
- At the Dapps layer, the appropriate application for each use case is enabling the actual interaction with the Smart Meters. Whether it is for example the participation of a prosumer in a market that is open for bidding (P2P energy trading), or the Demand Response management of a medium-size producer. In chapter 5, a case study using the mentioned architecture presented in Figure 4-6 will be provided.

4. 3 Methodology

The following is a description of the structure of all the work carried out to develop an energy gateway. The first is based on the definition of the challenges and problems we are trying to solve, then on the proposal of our prototype and, later on, on the definition of the components and technologies used. In a second phase, once the prototype is developed it is crucial to be implemented or simulated so that it can be tested and validated. Our final goal is to develop a low cost open source gateway that is capable of handling the transmission of DLMS/COSEM packet over LoRaWAN.

As already mentioned in the previous chapter, the reference architecture and functionality will be similar to the German SMGW which is developed and used only by the German energy sector (exclusive for German Energy System).

The methodology adopted to develop and to verify the functionality of our system follows strategy shown in Figure 4-7 and Figure 4-8.



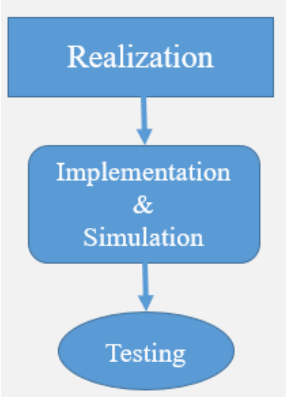


Figure 4-7: First Steps

Figure 4-8: Second Steps

4. 3. 1 Scenario Definition

The goal here is to define a typical gateway solution where DLMS/COSEM is portable over LoRaWAN. According to the existing challenges in the transmission of DLSM/COSEM by LoRAWAN, an interoperable solution should be developed to be implemented with the existing grid systems and that can help some countries to migrate their conventional grid to be smart and intelligent grid. Therefore, it is crucial to have a study of the DLMS/COSEM protocol in terms of specifications to test the possibility of transmitting such type of data over LPWAN technologies using IoT. According to the literature, we are familiar with the German system, which is a very advanced and recent system which is the main component of the German AMI system and it is crucial for the IoE enabling, in addition to the security enhancement provided by such a system. The decision to choose our prototype component and technology is made based on the existing challenges, metering and security requirements.

4. 3. 2 Implementation and Measurement

The goal here is to use the gateway already developed, adopted to international and European standards by testing its capability to transmit DLSM/COESM packets over LoRaWAN. Defining the scenario and the testing conditions means choosing some parameters to begin the simulation with and the design to be implemented. There will be three phases within the implementation:

- Metering data reading
- Metering data transmission
- Metering data visualization

Of course the focus will be on metering data reading since our main target is to be capable to transmit DLSM/COSEM over LoRaWAN.

We will use some tools to read and transmit the metering data.

Then, the second goal is to perform some simulation to verify the operation of the system. To ensure that the system works well and is compatible with the existing infrastructure, we had to conduct a serious real simulation over a period of time.

4. 3. 3 Evaluation

The main goal here is to evaluate the end results and expand our work to propose future improvements by integrating Blockchain technology which involves some security measures to avoid any data integrity. Finally, we will evaluate the system's performance in terms of efficiency and correct transmission without collision respectively. For the efficiency is about the advantages that are presented by deploying such a system. Efficiency can be given by the number of nodes which could transmit packets simultaneously.

4. 4 Proposed Architecture and Implementation of the Neighborhood Area Network

4. 4. 1 Design constraints

To convert the traditional energy meter to a smart meter, there are many constraints and challenges to take into consideration and should be predefined. The most important challenge is to design an interoperable module that can be easily integrated into the existing infrastructure and is able to transport the DLMS/COSEM packet over LoRaWAN. There is no standard defining the integration of LoRaWAN and DLMS/COSEM for smart grid networks. given the low power requirements, robustness, availability of LoRaWAN, and the specific device for smart meter applications, LoRaWAN has a great potential for deployment within the NAN network.

4. 4. 2 Design Modularity and Open-Source

In general, the modular design and open-source energy metering systems are intended for traditional meters' migration with flexible functionality. This will ensure the reliability, scalability, and modularity of the system to in order to adapt to any new features.

Some challenges and requirements need to be defined prior to defining the system hardware and software design. The module designed in this thesis is developed to add one of the smart features to the existing conventional meters. This system is user-friendly and can be used by researchers to test and study the best transmission scenario of DLMS/COSEM energy metering data packets over LoRaWAN taking into consideration both technologies' requirements.

4. 4. 3 Communication Protocol

For the communication network usually, a smart meter has two network interfaces: The one connected to the Home area network (HAN) where the commonly used technologies are Zigbee and Z-wave. The second network interface, the Neighbor Area Network (NAN) for communicating with the Network Operator where power line communication PLC and LPWAN technologies are used. In this study, we focus on the NAN area, where the module designed is developed to provide the Network Operator to read the energy consumption packets remotely and use them in a multitude of novel ways. Moreover, this module aims to transmit the energy consumption data via LoRa to a cloud server where it can be accessed and can be published to a blockchain for further certification and processing in the context of the P2P electricity trading platform.

4. 4. 4 Prototype Design and Implementation

The Lora module in this study is constituted of two main components: An Arduino platform and a LoRa shield that will allow the identification of the DLMS/COSEM energy consumption packet from the supported SM and transfer this data through a LoRaWAN gateway to the network server. The NAN Gateway is based on an iC880A-SPI extension board for a Raspberry Pi platform. This platform integrates Wi-Fi and Ethernet connectivity as well as sufficient memory resources for the microprocessor that runs a Linux distribution with 16 MB Flash and 4 MB of RAM. The LoRaWAN architecture is based on the topology of star-of-stars where the gateway plays only the role of a relay to transmit the data between the end device and the network server. The gateway is connected to the network server via the internet while the end-node is connected to the gateway via LoRa. Generally, end nodes communication is bi-directional, and all also support multicast communication for firmware upgrades over the air. The communication between LoRa node and the gateway can be performed using different frequencies and bandwidth.

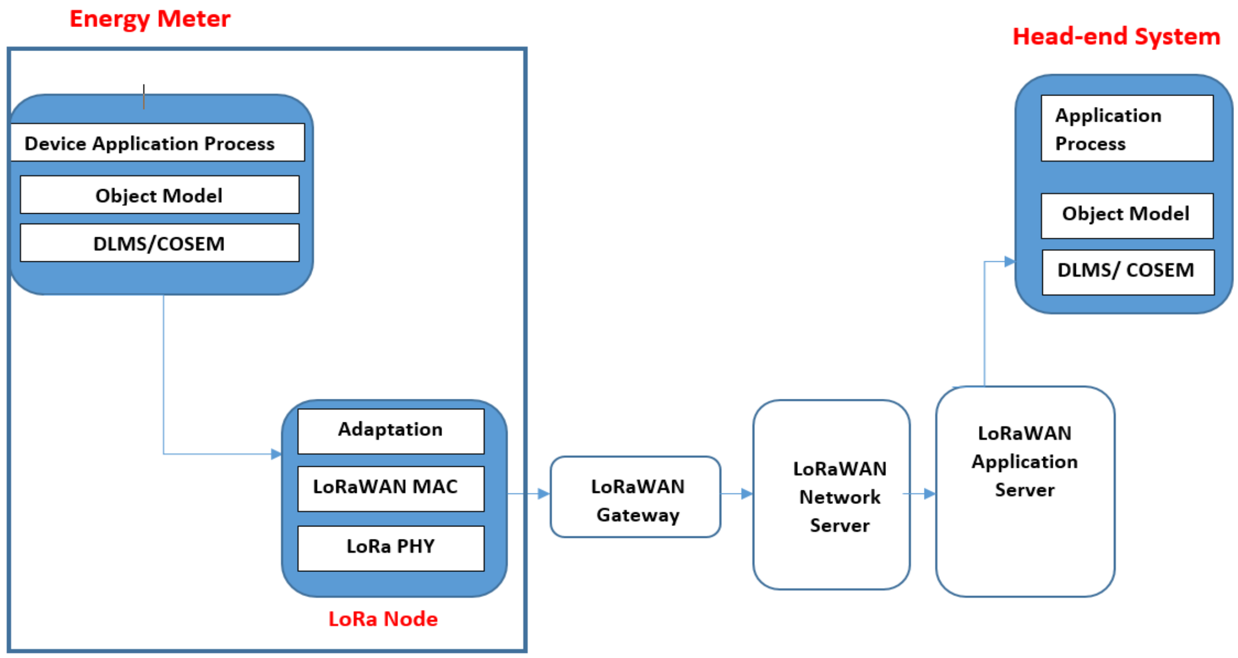


Figure 4-9: Proposed DLMS/COSEM over LoRaWAN Architecture

A typical LoRaWAN Gateway has been realized, based on the iM880B-L LoRa base station board from IMST GmbH integrated with a Raspberry Pi 4 used to retrieve the transmitted data and upload them to an application server, rendering them accessible for further processing. For the SM wireless connectivity Figure 4-9 an open-source platform based on the ATMega2560 microcontroller board has been utilized combined with an extension board (Dragino shield) for the LoRa Physical layers based on a Semtech SX1276 radio transceiver. Communication between the microcontroller and the LoRa transceiver takes place over a Serial Peripheral Interface (SPI). The Gurux DLMS/COSEM open-source library [21] has been used to generate the metering packets, where for example the function com_readAllObjects() initializes the connection, reads the logical device name, the clock, and the profile containing the data. Once all the relevant data are parsed, they are serialized and transmitted using the LMIC LoRaWAN library to the gateway using the LoRaSend() function.

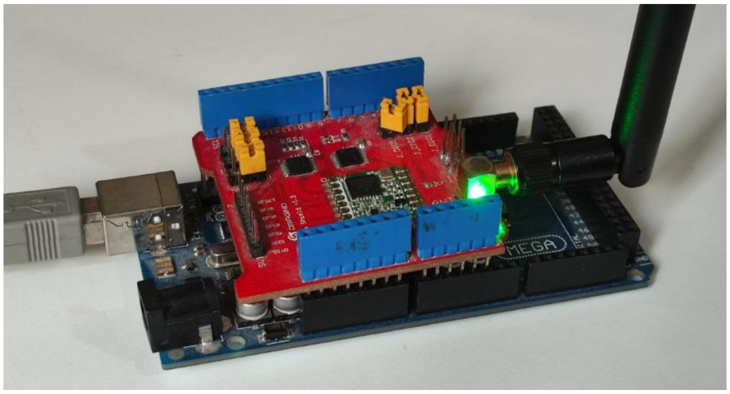


Figure 4-10: The DLMS/COSEM Compliant LoRaWAN Node for SM

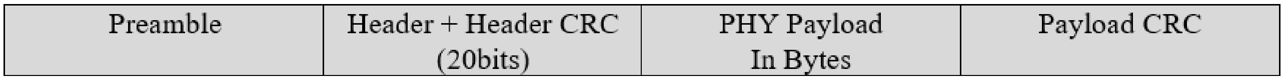
In the proposed architecture, the LoRaWAN data rate (DR), which is defined by the Spreading Factor (SF), and the Bandwidth (BW) while the maximum packet size extremely depends on the distance to the NAN gateway and are also defined in the specification for each region. For example, for the European 863-870MHz band, the maximum application packet size varies accordingly as is presented and summarized in Table 3:

- 51 bytes for the slowest data rates, with SF10, SF11, and SF12 on 125 kHz BW
- 115 bytes for SF9 on 125 kHz BW
- 222 bytes for faster rates, SF7 and SF8 on 125 kHz BW (and SF7 on 250 kHz BW)

SF	Bit Rate (bps)	Range (Km)	Time on the air (ms)	Max Payload (Byte)
SF10	980	8	371	11
SF9	1760	6	185	53
SF8	3125	4	103	125
SF7	5470	2	61	242

Table 4-3: LoRaWAN constraints

LoRaWAN protocol adds at least 13 Bytes to the application payload as shown in Figure 4-11.



Preamble	Header + Header CRC (20bits)	PHY Payload In Bytes	Payload CRC

Figure 4-11: LoRa Header

The constraints that we have taken into account in our tests are listed in the below section:

For DLMS/COSEM, the Application Packet Data Unit (APDU) of the maximum size of the packets of information may be negotiated according to the physical layer, however, the default value is 128 Bytes and the maximum 2030 Bytes. The APDU size of the commands packet that is exchanged to establish the connection is already mentioned in Table 4-2.

As we have seen in the previous section, the DLMS/ COSEM application packet can be transmitted with different transport and data link layer, where the added header size depends on the technologies used. In the case of TCP-UDP/IP the minimum header, size is:

- Wrapper overhead is 8 bytes
- UDP header is 6 bytes
- TCP header is 20 Bytes
- IP header is 20 Bytes
- MAC header 14 Bytes

Therefore, with the UDP option, the total header is equal to 48 Bytes, however with TCP total header 62 Bytes.

In the case of CO-HDLC the total header is equal to the LLD and HDLC header that is equal to 12 Bytes. Therefore, to meet the LoRa constraint regarding the maximum packet size, we had to choose the CO- HDLC as the communication profile to do our test.

On the other hand, one of the DLMS/ COSEM restrictions regarding transmission and reception time is that the maximum delay time for a response shall not exceed 500 ms, and in generally:

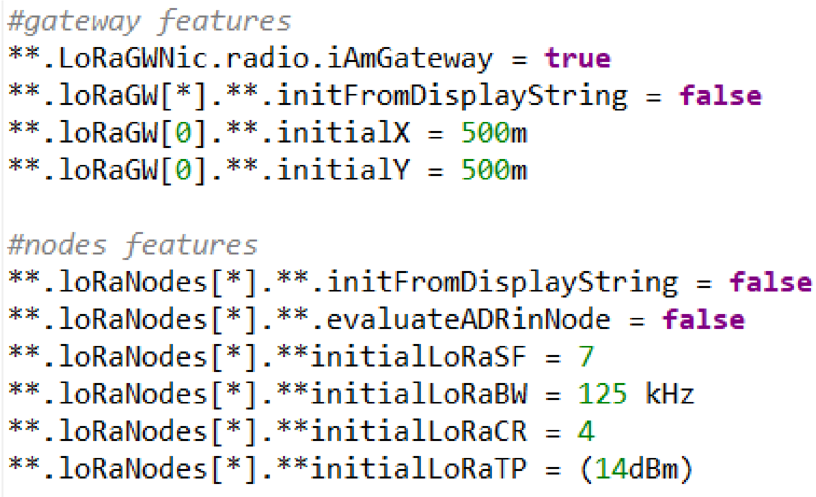
$Tr > Tr_{(theoretical)} + 2 * Tx_{(max)}$

Where Tr = Time for Response and Tx = Frame retransmission

In addition to the above requirement and knowing that energy packet measurement should be sent every 15 minutes, we had to choose the LoRa parameter so that the duty cycle, the time on the air met the requirements. Based on some calculations, we have taken as the default parameter for LoRa, an SF =7, the bandwidth 125 kHz, and the coding rate of 4/5.

The base stations are required to be equipped with a GPS receiver. The 1-pps (pulse per second) output of the GPS receiver is used to synchronize all the base stations with an accuracy of up to 12 picoseconds per second assuring a global timing reference. This is very important since for firmware Over the Air (OTA) updates over LoRaWAN class B must be selected for all the SM LoRa nodes that provide specific time slots for downloading the required updates.

The above scenario was simulated using the OMNeT++ simulator FLORA model. Ten smart meters from each building were simulated and deployed across a 1 km-by-1 km square typical urban area (which is a typical maximum size for a NAN area) with evenly distributed buildings in blocks of 20 m x 20 m. Packets are being transmitted every 15 minutes, using the default predefined values of LoRa with SF of 7, a bandwidth of 125 kHz, a Coding Rate of 4, and a Transmission Power of 14 dBm (Figure 4-12). The payload size has been adjusted to the predefined parameters shown in Table 4-2 for all the related commands/messages (SNRM, UA, AARQ, and AARE).



```
#gateway features
**.LoRaGWNic.radio.iAmGateway = true
**.loRaGW[*].**.initFromDisplayString = false
**.loRaGW[0].**.initialX = 500m
**.loRaGW[0].**.initialY = 500m

#nodes features
**.loRaNodes[*].**.initFromDisplayString = false
**.loRaNodes[*].**.evaluateADRinNode = false
**.loRaNodes[*].**initialLoRaSF = 7
**.loRaNodes[*].**initialLoRaBW = 125 kHz
**.loRaNodes[*].**initialLoRaCR = 4
**.loRaNodes[*].**initialLoRaTP = (14dBm)
```

Figure 4-12: LoRaWAN Energy Meters Simulation Parameters

The network consists of the SM nodes, the LoRa Gateway, the gateway router (gwRouter) for the internet interface, the network router (nsRouter), and the network server (networkServer) objects as shown in the Figure below. The Smart Meter nodes transmit data to the LoRa Gateway (LoRaGW), which then transfers data to the network server via the gwRouter, the internet and the nsRouter object as shown in Figure 4-13.

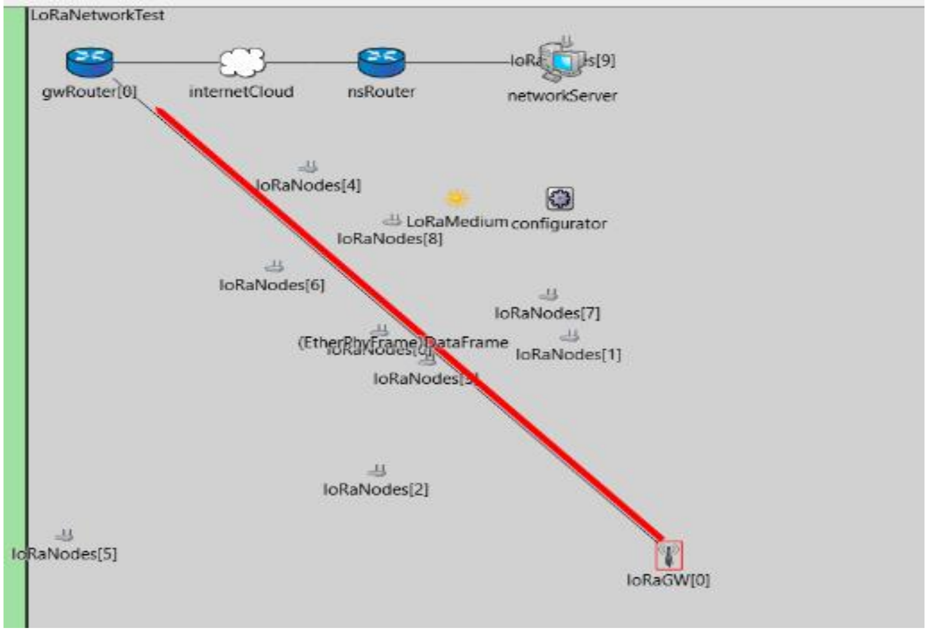


Figure 4-13: OMNeT++ Simulation topology of the LoRa nodes

4. 5 Results and Discussion

The feasibility of a LoRaWAN enabled DLSM/COSEM integration was investigated and discussed about its benefits and demonstrated by experimental implementation. The proposed prototype is tested under the following experimental conditions:

- Class B LoRaWAN Node (for bi-directional communication)
- Simulation duration of 10-days
- 1000 smart meter devices
- Data aggregated on an 8 channel LoRaWAN gateway.
- Gateway deployed at the center of the setup area
- Smart Meter transmitting of the EU863-870 frequency band.

- Channels utilized: 868.10MHz, 868.30 MHz, 868.50 MHz, 868.70 MHz, 868.90 MHz, 869.10 MHz, 869.30 MHz, and 869.50 MHz
- A random (uniform distribution) start of transmission time for each node for the transmission period of 900 seconds
- The sensitivity of each LoRa modem was set at a typical -137 dBm
- Isotropic antenna models on all nodes
- Urban environment path loss
- Data on the gateway is forwarded to an application server to be made available

During the scenario 1000 smart meter nodes were simulated in a LoRaWAN Class B configuration, divided into six groups of 125 meters, transmitting to eight different channels EU863-870 LoRaWAN. These SMs were configured to transmit at an interval of 15 minutes, with a uniform distribution of messages during that period. The 15 minute sampling period is suggested by the European Union as the standard interval for energy smart metering.

The simulated system transmitted 96,000 messages per day, for a total of 960,000 messages in 10-day simulation period. The RSSIs of the received messages were ranging from -105 dBm to -128 dBm, a mean of -121 dBm, and a standard deviation of 4.78 dBm.

A typical concern presented in LoRa or LoRaWAN configurations and systems is related to the possible collisions due to high channel usage (Figure 4-14). In LoRa modulation, packet collisions occur when at least two packets are transmitted at the same time, thus overlap, and use the same LoRa parameters, such as the same Bandwidth (BW), central frequency, Spreading Factor (SF). The capture effect found in LoRa modulation offers the advantage of successfully receiving a packet with a higher power level of at least 6 dB that is transmitted simultaneously with another and still being able to decode it. The probability of a collision depends on many factors, such as the number of nodes, the transmission interval, the selected Spreading Factor, the transmission power (TP), etc.

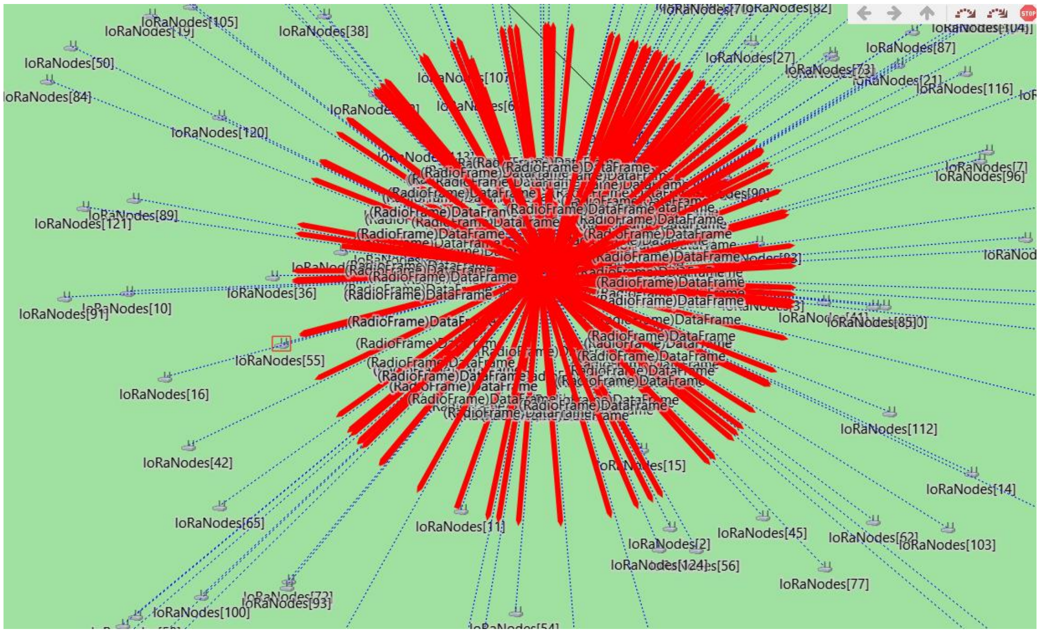
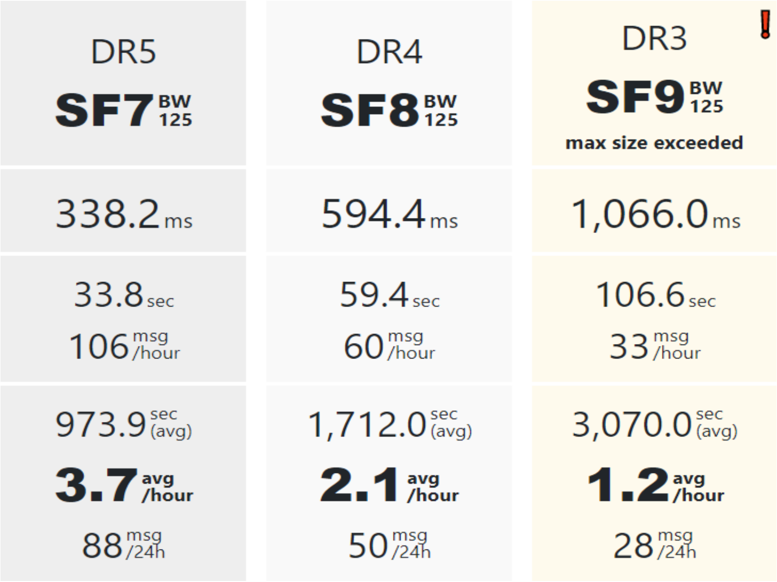


Figure 4-14: Multiple Nodes Transmitting Simultaneously Resulting in Collisions

To minimize collisions, an experimental timing protocol to variate the interval between the DLMS/COSEM messages has been implemented, using the uniform function of OMNeT++, which returns a random variate with uniform distribution in the specified range. Additional mechanisms can also be implemented, such as Listen Before Talk (LBT) for each LoRa node, to check that the specific frequency band is not utilized by another node before transmitting. However, such a mechanism consumes additional power from the node and is not used by in a standard LoRaWAN configuration and thus has not been simulated [20].

The simulation results show that, by increasing the number of channels used to eight, as well as adopting the aforementioned timing protocol, only 0,8% of the messages transmissions collided, resulting in a 99,2% success rate. This number of collisions is considered acceptable and within the typical design limits in LoRaWAN networks. With a 0.8% collision rate, the system will be fully functional in a high-density Smart Meter area, such as the simulated urban area, while fully complying with the duty cycle requirements and regulations. In any other area, with a lower population density, there will be fewer SMs transmitting and receiving data resulting in even fewer collisions.

Taking into consideration the aforementioned results, we have successfully verified the feasibility and the functionality of the proposed DLSM/COSEM compliant implementation over the LoRaWAN architecture. Other experimental scenarios either did not meet the timing constraints of the maximum transmission time of 500 ms, or the European regulations for the duty cycle. For example, by changing the LoRa Spreading Factor parameter, the time on-air will be directly affected. Time on air is the time to transmit a packet of data. A Spreading Factor (SF) is specified for each transmitted packet of data, the SF is equal to $\log_2$ (Rc/Rs), where Rc is the chirp rate and Rs is the symbol rate. Therefore, there is a compromise that has to be made between the communication range and the Spreading Factor. When the SF is higher, the data rate is lower and the communication range will be longer. With different SFs the simulation failed to meet the DLMS/COSEM transmission time. As shown in Figure 4-15, when using an SF equal to 8 for a packet with a payload of 200 bytes, the airtime needed for a complete DLMS/COSEM sequence becomes equal to 594,4 ms. As a result, the transmission violates the 500 ms time limit and the four-transmissions per hour quote to meet the 15-minute sampling period. Only by selecting a Spreading Factor of 7 both the required transmission time (max 500ms) and the required duty cycle were met.



DR5 **SF7** BW 125	DR4 **SF8** BW 125	DR3 ! **SF9** BW 125 **max size exceeded**
338.2 ms	594.4 ms	1,066.0 ms
33.8 sec 106 msg /hour	59.4 sec 60 msg /hour	106.6 sec 33 msg /hour
973.9 sec (avg) **3.7** avg /hour 88 msg /24h	1,712.0 sec (avg) **2.1** avg /hour 50 msg /24h	3,070.0 sec (avg) **1.2** avg /hour 28 msg /24h

Figure 4-15: Time on Air variation with different Spreading Factors

The adoption of the above scenario allowed for the transmission of DLSM/COSEM message sequences without violating the imposed payload constraints while at the same time meeting the transmission time requirements. However, an additional delay has been detected in the implemented system which is related to the processing speed limitations of the Arduino platform as well as to the network latency during publishing the generated data packets via the TCP/IP stack to the network server. This delay is in the order of milliseconds and can be further minimized by using a more advanced microcontroller with a faster CPU and an embedded high-speed network modem. In all cases, implementation is in accordance with European Union directives on smart energy metering.

4. 6 Conclusion

The ongoing effort to transform the energy sector to the Internet of Energy is impacted by the wide variety of communication technologies and data exchange protocols. In this chapter, we discuss the advantages of adopting low-cost IoT solutions and Smart Metering communication protocol standards targeting the renovation of existing electricity Grids to Smart Grids with peer-to-peer electricity exchange capabilities. Towards this scope, in this chapter we proposed a Smart Grid architecture based on the DLMS/COSEM energy-metering communication standard and LPWAN communication technologies, while a Blockchain layer enables the smart-metering data integrity for electricity trading.

In this chapter, we have designed, simulated, and implemented a case study using open-source hardware and software components for the two lower layers of the proposed architecture focusing on the Neighborhood Area Network (NAN) electricity trading case study. Peer-to-peer electricity trading in a NAN was selected because electricity exchange between producers and consumers are essential for a massive injection of renewable energy sources in the modern Smart Grids. For this specific case study, an experimental setup was developed implementing the communication between the SMs and the NAN Gateways using open-source hardware and software components. Both the implementation and the simulations tested the successful transmission of the DLSM/COSEM message sequences without violating the required payload constraints while respecting the transmission time requirements imposed by EU norms and practices.

The proposed implementation of the DLMS/COSEM Energy Metering Standard on LoRaWAN NAN Infrastructure can facilitate and encourage the deployment of other third-party added-value services, such as the global manipulation of multiple distributed energy sources or loadings to support scenarios such as virtual power plants, demand-side control for load-shifting, and energy curtailment for power savings through consumer awareness and engagement. And of course, the long-anticipated peer-to-peer energy trading for distributed small prosumers, including the encouragement of localized transactions.

The proposed global architecture can be easily adopted and widely implemented by local communities due to its low-cost requirements, interoperability of standards and compatibility of existing infrastructure. As such, it can be useful to the scientific community and utilities to test and evaluate smart meter implementation strategies based on IoT technologies.

In the next chapter, and in order to add security features to the developed gateway, the integration and utilization of new technology such as Blockchain will be tested. Blockchain will provide a secure data integrity feature, we will study the improvements that can be added by such technology in terms of security and enablement of P2P energy trading.

Chapter 5 : Blockchain and Secure Element Combinational Approach Applied to Energy Smart Meter Gateway

5. 1 Introduction

Today, more than ever, the upward trend of decentralization of information technology (IT) over the last decade as well as data processing near the "edge" of the network (Edge Computing) seems to be approaching the time of a complete independence from a single central system that collects, controls, and ultimately consumes data. Devices (or "Things") that make up the modern Internet of Things utilize, adopt and integrate architectures, features and capabilities (i.e., Raspberry Pi[1], ESP32[2], Single/Multi-Core ARM[3] or RISC-V[4] based Microcontroller Units - MCUs & Microprocessor Units - MPUs etc.) which are constantly seem to approach those of much more powerful systems. It is therefore justified an intense global research activity in the fields of Decentralized and Distributed Systems under the prism of "Constrained Resources Computing Systems" that are usually found as clients - at the lowest level - in IoT environments.

Computing capabilities and data storage tend to move closer to the data generation site, with the ultimate goal of improving response times and saving bandwidth. Edge computing and the speed at which it develops make an extremely important contribution to the overall effort to decentralize these networks. Such a network will ideally consist of heterogeneous systems, which may not already be registered in the network, but must be quickly connected to it in a secure manner.

In this cutting edge period, the boundary between the physical and the digital worlds is narrowing with the growth of ICTs. As more and more things are digitalized, numerous conventional notions of the physical world are being reconsidered. This re-evaluation redefines these conventional ideas, often making them more comprehensive concepts like signatures, crypto-currencies, fingerprints and transactions are examples.

Automatic data transfer/transaction which is one of such traditional concept, has been completely redefined. While conventional distributed databases resolve the data integrity issue, the complex issue of transaction security remains a difficult one to resolve. The Introduction of Blockchain (BC), which is a new paradigm that has the potential to overcome security and trust challenges for IoT platforms, as a distributed data base partially solves the issue. Blockchain alone by itself is not able to completely secure a transaction because it is only to guarantee data immutability while in most cases the data has to be secured at the point of generation. Furthermore, due to its significant overhead blockchain is not able to penetrate to lower levels in a system. Therefore, to fill this gap we propose the use of Secure Elements (SE) to build a "root of trust", and to give IoT devices trusted computed resources to generate cryptographic signature, following the secure by design model. These two technologies combined help overcome the obstacles associated with the use of a unique technology and used as the basis of our decentralized and secure end-to-end IoT system that we will apply and test it in Energy Smart Metering gateway to enable local P2P energy trading.

While renewable energy is developing rapidly as part of the energy revolution, the structure of energy systems is gradually being decentralized. Nowadays, blockchain-enabled distributed energy resources, like solar panels, photovoltaic (PV) systems and microgrids that transfer consumers into prosumers who are active users that can sell their excess of energy to the grid, is growing. In this context the new players, such as prosumers with low capacity of energy production that does not allow them to participate in energy market, could organize a P2P local energy trading without the intervention of any authority or third party. However, in order to deliver an effectively secure P2P energy trading, Local Energy Markets (LEMs) require a method to implement original and secure information and communication technology. Blockchain combined with Secure Element (SE) and modern Smart Meter Gateways (SMGW) could help the existing energy systems to become more decentralized, secure, smart, and interconnected.

The growing complexity of the balance of existing infrastructure and data security requirements related to electricity interchange and billing must be digitized. An intelligent smart metering system and a Smart Gateway (SMGW) which is placed as a relay between Smart Meters (SM), Consumers and External Market Participants (EMP) can provide a secure way of making this desirable digitization feasible. The purpose of this work is to examine and test the implementation of a blockchain and secure element based SMGW, as an enabling technology for energy digitization.

5. 2 Introduction to Blockchain

Blockchain, in simple terms, is a chain of blocks (containing information) that are connected to one another through cryptographic functions creating a solid chain. This gives the ability to record transactions via a secure and verifiable way without need for a third party [5]. In general, when creating a new block, only the hash from the previous block is included.

Blockchain as an idea and model goes back almost three decades. The block concept was first implemented and introduced in 1990 by Haber et al in their work entitled "How to timestamp a document" [6]. However, blockchain has been well known and implemented in 2008 by bitcoin [7], which is the first blockchain based cryptocurrency.

In its simplest form, a blockchain block consists of data segregated in multiple tiny entities known as transactions, a hash of the previous block. Blockchain structure is presented in Figure 5-1. BC offers immutability by securely saving ledger copies on all blockchain active nodes. The different existing consensus algorithms (like Proof of Work (PoW), Proof of Stake (PoS) are used to achieve coherence. Blockcahain active nodes create the P2P network and a communication protocol is deployed between them to circulate information.

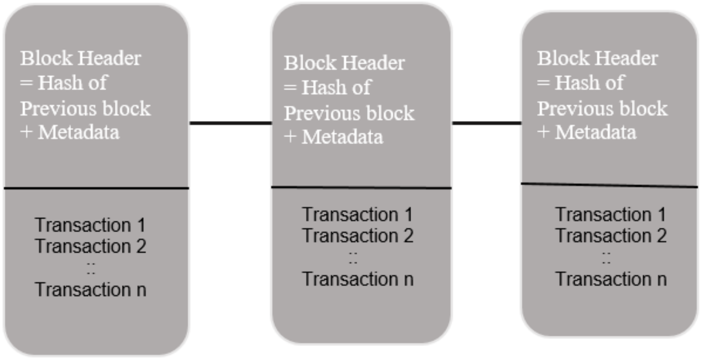


Figure 5-1: Blockchain Structure

Different blockchain classifications are presented in [8]. Actually blockchain can be split into many categories based on different parameters like protocols, permissions and domain of application etc. Based on permissions, blockchain is divided into two main types i.e. permissioned and permissionless. In a permissioned blockchain, some permissions are pre required to get access/ read/ write on the blockchain, however for permissionless blockchain no permissions are required. Figure 5-2 represents the different classifications within the permission category.

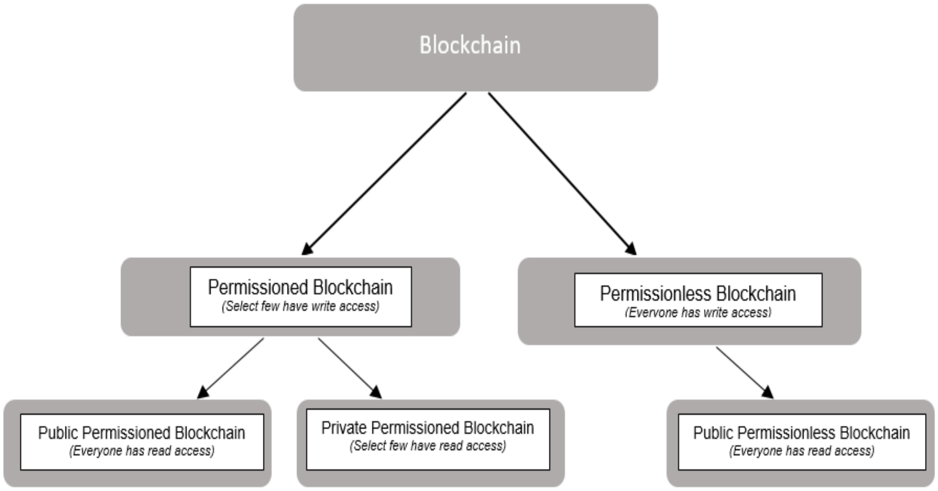

Blockchain
Permissioned Blockchain
(Select few have write access)
Permissionless Blockchain
(Evervone has write access)
Public Permissioned Blockchain
(Everyone has read access)
Private Permissioned Blockchain
(Select few have read access)
Public Permissionless Blockchain
(Everyone has read access)

Figure 5-2: Permissions based Blockchain

DLT and Blockchain Emergence Distributed Ledger Technology (DLT) can be seen as a database that shares data between computers and users worldwide. Contrary to the classic approach of centralized servers and authorities, it enables a decentralized environment with many advantages that are not yet discovered or fully utilized yet. For example, most companies today use a central database with a fixed location. The main disadvantage of this is that there is only one point of failure of the system. As this point fails, the entire system will not be active until this point returns to operation. On the other hand, a distributed ledger exists between many sites and nodes and is governed in such a way thus allowing access and providing the ability to make changes by multiple participants in a network without the need of centralized authorities. Since the first appearance of Bitcoin, other cryptocurrency also emerged with the most recognizable among them being Ethereum. While the crypto domain is growing at a significant rate, a lot of literature and conversation around them is also growing due to the underlying technology that is called Blockchain. Blockchain enables participants who may not be familiar with each other to do business directly and securely. — In theory, without the need for a lawyer, bank, broker, or government to negotiate the transaction.

5. 2. 1 Blockchain and Data Reliability

Blockchain Wallets any computer (participant) that connects to a blockchain network is called a node. Most of the time nodes offer wallet capabilities which are required to carry out blockchain transactions, therefore another way of describing nodes is "clients that supply wallet functions". There are two basic types of nodes as shown in Figure 5-3, (a): A Full node contains a copy of the entire blockchain’s history, including all blocks created and all transactions ever made while a Light node does not need the whole blockchain to be downloaded. Instead, it downloads the block headers only to validate the authenticity of the transactions. Because of this, light nodes are easy to maintain and run. Lightweight nodes use a method called Simplified Payment Verification (SPV) to verify transactions. Some other sub-types of Full nodes which are namely Pruned and Archival also exist, with the latter having also Master, Mining, Staking and Authority as sub-categories.

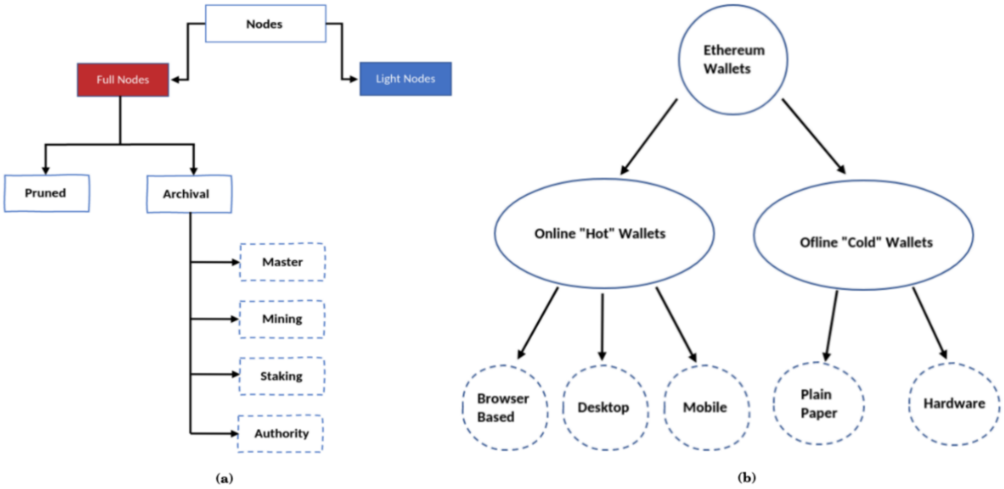


Figure 5-3: (a) Node Types, (b) Wallet Types

A wallet briefly is used to interact with a blockchain network. Its main functions in general could be:

1. Generate and secure private and public keys
2. Scan the Blockchain for relevant transactions

- In a Full node wallet, the whole chain needs to be downloaded and all blocks and transactions needs to be validated (signatures, other protocol rules).
- In a Simplified Payment Verification (SPV) wallet which is also considered as a Light node, there is no need for fetching the whole chain but only relevant information from other peers.

- There are also other types of wallets, based on third party APIs which are used to communicate with Light or Full nodes and get information about certain addresses.

3. Sign and broadcast new transactions

There are 2 types of crypto wallets, as shown in Figure 5-3, (b) for internet connectivity, namely hot and cold. Hot wallets require internet connectivity and are also called online wallets, while cold wallets do not require an internet connection and are also called offline wallets. Cold wallets are safer and are not vulnerable to network attacks since a physical interaction is required to get access on the keys, observe a key generation or create/sign an unwanted transaction. Wallets can be further classified according to the method, location of storage and functionalities: (i) hardware, (ii) software (desktop, mobile or web), and (iii) paper wallets.

The most significant part of a wallet as an entity is the private keys storage and safety from non-authorized usage (i.e., some other person having access on its assets). In the crypto currency domain, there is a famous sentence on this subject: "Not your keys, not your coins" which means that anyone who has access to a wallet's private keys can spend its funds. Thus, the critical functions of a wallet from a security perspective are those of securely generating key pairs (public, private) and securely storing those keys (public and/or private).

5. 2. 2 IoT and Blockchain Convergence

The combination of DLTs (Distributed Ledger Technology) with the IoT has also been widely investigated in recent years in the international literature. Despite this relatively new direction, a variety of views and results have already been created and continue to grow [2] [3] [4] [9] [10] [11]. From the conclusions of most publications, it seems that several advantages could be obtained in terms of modern problem solving, but also modern solutions to meet new needs, allowing the realization of actual Cyber-physical Systems (CPS) which in turn, will significantly improve in a wide range of everyday tasks, the human living standards

5. 3 Secure Element Introduction

Usually, a Secure Element (SE) [12] is based on a programmable micro-controller MCU that resists tampering and provides a Trusted Execution Environment (TEE), and Trusted Storage

Environment (TSE). In general SEs are tiny in size (25 <<2) and produced to provide security capabilities like digest functions (SHA1, SHA2, MD5, etc.) and cryptographic functions (Elliptic Curve Cryptography (ECC), Rivest-Shamir-Adleman Algorithm (RSA), Advanced Encryption Standard (AES), etc.). To accelerate the execution of these operations, a crypto-processor is integrated in the SE.

The SEs specs are usually as listed: it comes with less than 1 MB of ROM (200-500 KB) and less than 15 KB of RAM [13]. With specs, a SE can save up to 5 applications that are named codelets/applets since they are too small apps executing a particular function.

More than ever, SE is becoming widely used and in different fields like payments for credit and debit cards, telecommunication for SIM cards, IoT [14] for authenticity, identification and verification and finally it was used to provide a root of trust in blockchain-IoT platforms [15] and it contributes to the application in different ways such as secure boot, secure messaging and DTLS.

In addition, there are two well-known SE categories: SEs that are based on Multos(Multi-OS) [16] and SEs that are based on Java Card. Both Java Card and multos are secure elements Operating systems. Multos SE application known as codelets while the Java Card SE application are known as applets. Both SE categories are well known in the commercial context. However, Riddle&Code company has introduced their secure element 2.0 which is part of their product range "built for Blockchain" that allow secure storage of the digital identity (which is the private key) on a given device via a hardware and software combination. Riddle&code secure element 2.0 was considered in our testing and simulation case study.

Since the design of Multos SE is based on the concept of security by design, it requires a specific programming certificate known as the Application Load Certificate (ALC) however for Java Card based SE, the same rule is not applied, the installation and the update of the applets cannot be done without a key. The use of such a key will provide an additional security layer to prevent any unauthorized programmer from compromising the security of SE by downloading any malicious code to the SE. Since the symmetric key rule is not applicable with Multos SE, as is the case for SE based Java Card, then there is a possibility to be remotely programmed even is an unsafe environment. For Riddle&code SE 2.0 it cannot be programmed remotely, it is programmed on site and once configured no new changes can be done.

Since SEs are a significant category of security applications, they are certified under the Common Criteria-Evaluation Assurance Level (CC-EAL). EAL1 is the lowest certification level where EAL7 is the highest. However, under the EAL7+ level, which higher than EAL7, exists some SE.

The mode of use of SEs is either standalone secure MCU or used in combination with a complex system like Hardware Security Module (HSM). Depending on the security level or whether or not the SE supports Public-Key Cryptographic Standards PKCS, prices change significantly. The majority of secure elements are compatible with the Application Protocol Data Unit (APDU) over serial or NFC interface. However, some secure elements support the Serial Peripheral Interface (SPI) or the Inter-Integrated Circuit (I2C). In summary SE characteristics:

1. Supports Trusted Execution Environment TEE
2. Based on a crypto processor and crypto storage
3. Has some memory limitations
4. Support I2C, SPI
5. Certified by CC-EAL

IoT and Secure Element Convergence

The combination of SE (Secure Elements) with IoT has recently been studied in some international literature. SE has been tested and used on a large-scale in different domains like payment (chip-based cards), Telecommunication (SIM cards), identification papers (biometric passports), IoT [14] (for identification, authentication, certification, verification) and it is also implemented to create a root of trust in Blockchain-IoT systems [15]. The conclusions of most publications suggest that there are a number of advantages to SE in solving modern problems.

5. 4 Internet of Energy

The energy industry has always been straight forward. For years, it has been based on centralized systems of generation, storage and use with the energy provider in the middle. However, the situation has changed notably. The rise in global technology and the shift to renewable energy from different decentralized resources has shifted the energy balance of centralized energy suppliers to a large number of active prosumers. Prosumers centricity has introduced new challenges for all active members in the energy network. The new challenges can be presented as follow:

- Real-time billing
- Gives the consumers new roles
- Provide energy supply stability
- Response to consumer's demands

Decentralization, which is necessary to face all these new challenges, needs trust and security. The implementation of a trusted smart meter gateway (presented in the following section) at the prosumers premises is the solution to provide a reliable and secure system to meet the above challenges.

With the growth of ICT application, the connectivity between the physical world (like machines and devices) and the human world becomes much greater, which introduces the concept of energy digitalization. Energy digitalization is changing the way that energy is generated, distributed, used and sold. The introduction of IoT and blockchain technologies in the energy sector enables the production and consumption of energy and make it possible for consumers to benefit from the use of green energy.

Blockchain and Internet of Energy (IoE)

Electricity networks worldwide, were initially built for a one-way power flow, with fiat money flowing in reverse. Producers were expected to be larger than consumers, but given the potential growth of prosumers, many challenges are currently under consideration. Rebuilding power networks is a difficult challenge, but restructuring the electricity market is a totally different challenge.

Blockchains in general provide a distributed network, which in turn reduces the costs of installation and maintenance of centralized servers, data centers and networking equipment. This is done by distributing computation and storage requirements among all blockchain nodes establishing the network. This allows participants who may not be familiar with one another to do business directly and safely. Smart Contracts that contain the corresponding rules, basic interactions requiring an intermediary to be done are now possible without the intervention from of a legal representative, bank, broker, or government employee to intercede a deal.

Blockchain will most probably disrupt the energy sector, in the following individual areas[17]:

- Finance enhancement within distributed energy sources and battery storage.
- Solution to the split-incentive problem with multi-owner properties.
- Optimized utilization and increased value of network assets.
- Affordable and easier access to modern energy markets even for entry level prosumers.
- Enablement of a decentralized platform for generating and distributing power.

According to[18] there are seven different research domains regarding blockchain and energy:

- The decentralized energy markets
- Micro grid and Smart grid
- Energy internet
- Smart contract
- Peer-to-peer
- Renewable energy
- Electric vehicle

In our case we exchange data between smart meters and a gateway and then upload them in the blockchain network. While generating, signing, and sending transactions from constrained resources devices like a microcontroller based embedded device plugged in our scenario’s smart meter and other smart meters also (e.g., for other manufacturers – other countries’ standards) is a task that needs sophisticated engineering, other methodologies can be used to allow the Smart Meter to send measurements to a blockchain network. In general, any device able to execute blockchain cryptography algorithms needed can directly utilize the benefits of smart contracts, thus eliminating the need for centralized gateways and points of failure.

5. 5 Trusted Energy Smart Meter Gateway

The trusted energy smart meter gateway, is the foundation of a decentralized energy marketplace.

It represents the interface between the physical world (PV, smart meter) and the energy market place. It enables the energy digitalization. Such a gateway connected to a SM enables a trusted and secure energy trading system and gives small producers the ability to trade energy and exchange values.

This gateway is equipped with a cryptographic component. This device provides the trusted gateway with the possibility to uniquely assign identity to the SM and certify it to the blockchain. After this first attestation, the component generates a digital twin to the SM and provides the gateway with an account-agnostic agreement capability. Each fraction of additional power generated on this SM is recorded, signed and published to the blockchain.

This trusted gateway functionalities can be summarized as below:

- Gives a single digital identity to the SM and certifies it to the blockchain
- It gives transactional capabilities to the SM
- The connectivity between the gateway and the SM, combined with cryptographic device allows prosumers to record and verify the extra generated power to the blockchain.

5. 6 Combinational Approach Applied for P2P Energy Trading

In the context of the local P2P energy trade, prosumers can sell their extra energy produced by their RES to the neighborhood. However, such a system requires a decentralized trusted and secure infrastructure in order to avoid any data alteration between the point of generation and the destination. To meet these requirements, we apply our combined blockchain-SE approach to suggest a new open source trusted energy smart meter gateway that will be node in the blockchain. This combination will improve the system transparency, integrity, root of trust, non-repudiation by using the SE along with total decentralization immutability by using blockchain. In this approach we have used the BigchainDB blockchain, which is a scalable open source database and supports multisignature transactions, smart contracts and a secure element developed by

Riddle&code company. Further, through our simulation we have successfully demonstrated and tested the realization of such an approach, and we have presented a secure trusted SMGW open source to enable local P2P energy trade.

5. 6. 1 BigchainDB

BigchainDB is a software that combines both blockchain and data base properties. It was first announced open source in February 2016. Later, it has been significantly improved to reach the version 2.0 that was implemented in our simulation. The main particularity of this version is that now it is based on the Byzantine fault tolerant (BFT), So, in case until the third failure of active nodes, the system will always be able to agree on how to remain functional. This version was designed to meet the following goals:

	Blockchain	Distributed Database	BigchainDB
Decentralization	X		X
Byzantine Fault Tolerance	X		X
Immutability	X		X
Owner-Controlled Assets	X		X
High Transaction Rate		X	X
Low Latency		X	X
Indexing & Querying of Structured Data		X	X

Table 5-1: BigchainDB 2.0 Enhancements

BigchainDB as a blockchain database, it is becoming a complementary to another decentralized framework, like smart contract based blockchain (for example Ethereum or Hyperledger) or like data exchange protocols based decentralized systems (Ocean Protocol), and it is also compatible with centralized computing framework. Figure 5-4 shows different ways to use the BigchainDB different technologies stacks, starting from the left with a centralized cloud computing based environment where BigchainDB can be used to gain some decentralized features to the left where BigchainDB it can be used in a fully decentralized environment.

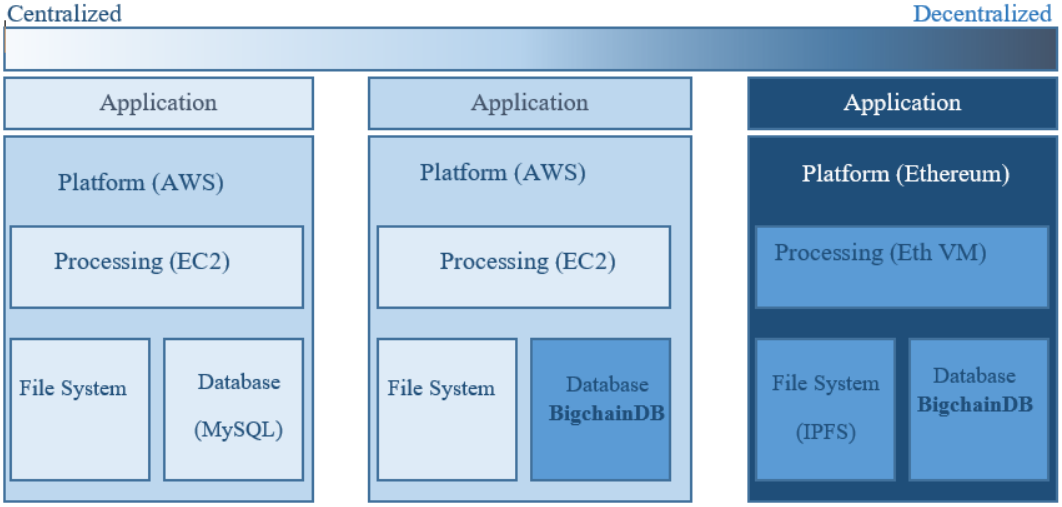


Figure 5-4: BigchainDB Ways of Usage

How BigchainDB 2.2.2 Works:

To be compatible with BigchainDB transaction specs version 2.2.2, a bigdchaindb transaction is a JSON string. Spec v2 describes the instructions for how to create and publish a transaction, in fact, a checklist must be verified to confirm the validation of a transaction and the details of the cryptographic functions that have been applied. To build a valid transaction, then you have to use BigchainDB drivers, once the transaction is created it can be sent to the network by using the BigchainDB HTTP API (the transaction will be in the body of http request where this request can be sent to different nodes within the network). When the transaction arrives at the node, it arrives at the web server in the node where all the incoming web requests must be redirected. The web server has an interface that permits python based application to communicate with it. BigchainDB usually use a web application to redirect the request to python’s method for processing that endpoint. This method verifies the validity of the transaction, in case of no validation an http response error code 400 is sent, however in case of validation, the transaction is converted to Base64 and placed in a new JSON string, then this string is sent to the local Tendermint instance within an http post request this request utilizes the Tendermint broadcast API. So when the transaction arrived to the Tendermint it will run via CheckTx, if this function return true the transaction can be then broadcasted to other nodes and finally placed in a block.

5. 6. 2 Riddle&Code Secure Element

As already mentioned what is the most important about crypto and crypto currency is to protect and save your keys in a secure way which means not saving them on a cloud or an email or on your USB without encryption. However, to enhance the overall security of the key host the direction nowadays is to integrate hardware secure modules that is responsible of storing critical data in an unconventional way. Hardware functionality may be described as follows:

- Random Generation Number (RGN) which is a main function for key generation
- Secure Storage where the keys are stored and hidden inside the EEPROM where it is impossible to retrieve the secret
- Signature on Chip
- Encryption and Key Derivation can be done on chip

With the growing need for IoT for hardware level security, some special hardware and software shift the trust layer from user to kernel level, making a separated and hard to manipulate environments for critical data operations. And since crypto-accelerator chips are specifically developed for this kind of operation, they are powerful, faster and more effective than their software version. These characteristics totally fit into the IoT concept since IoT devices are battery based and have low computational power.

Secure elements have been used in different fields like:

- Hardware crypto currency wallet
- Payment system (PIN card)
- Secure boot
- Secure messaging
- Authenticity validation with TLS handshake

Riddle&Codes has developed a Secure Element that can be inserted to different types of devices to provide them a secure identity. Riddle&Codes has different types of secure elements as below

- The universal edition that is based on Atec 608A and a Crypto storage.
- IoT edition that is based NXP SE050 and a Crypto storage.

What is the Secure Element being used for and how it works?

As previously mentioned, a secure element is a chip which is protected by the design of illegal access and it is utilized to execute a restricted set of applications and also it is used for storing sensitive and cryptographic data.

The Riddle&Code Secure Element is composed of a crypto accelerator to generate a digital identity which is the private key that never ever gets out of the crypto accelerator. However, the public key can, for sure, be retrieved. It also has an encrypted EEPROM that is used for safe data storage. To interact with the secure element there are some Software Development Kit (SDK) documentation. These documentations include different development environment set up that describe how you can connect a secure element either to an RPi or an arduino.

5. 7 Combinational Approach Implementation

5. 7. 1 Scenario Definition: End-To-End Implementation Architecture

First, it needs to recognize that security in general is a complex and constantly evolving issue. In this work a proof-of-concept is described in which a crypto wallet is implemented in a gateway Figure 5-5, (b) that is the middle device between smart meter and the local market. This trusted gateway is composed of a Secure Element (is composed of a **Crypto Accelerator** Microchip 608A and **Crypto Storage** Microchip ATAES132A) and RPi.

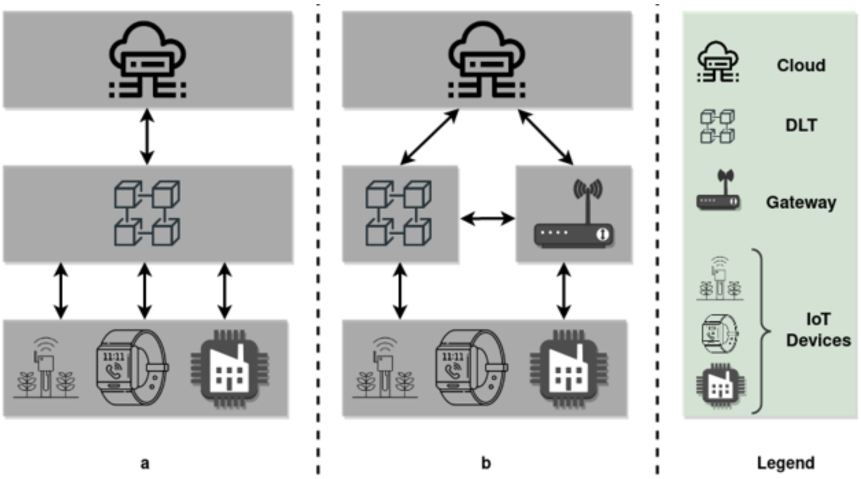


Figure 5-5: DLT and IoT Integration schemas (a) Without a Gateway Device, (b) With Gateway Device

In our PoC the trusted gateway, that is based on a SE and RPi, at the setup phase will generate a pair of keys to identify the SM to the blockchain (those keys are generated by the SE element that is capable to generate up to 15 pairs of keys per slot, once the slot is locked you cannot regenerate any new pair of keys for the locked slot). The trusted gateway will read the metering measurement from the SM and will send this data to the Secure Element, at its turn the SE (stores the private key used for signing the data) will sign the data by the specific generated private key, then the SE will send back the data to the RPi. The Pi which connected the blockchain (in our case BigchainDB which is capable to store encrypted and signed data) is now responsible for creating a transaction that contains the metering data and publishing the data on the blockchain. The ownership of this data can be transferred to another user on BigchainDB by transferring assets. The Figure 5-6 shows the data flow diagram.

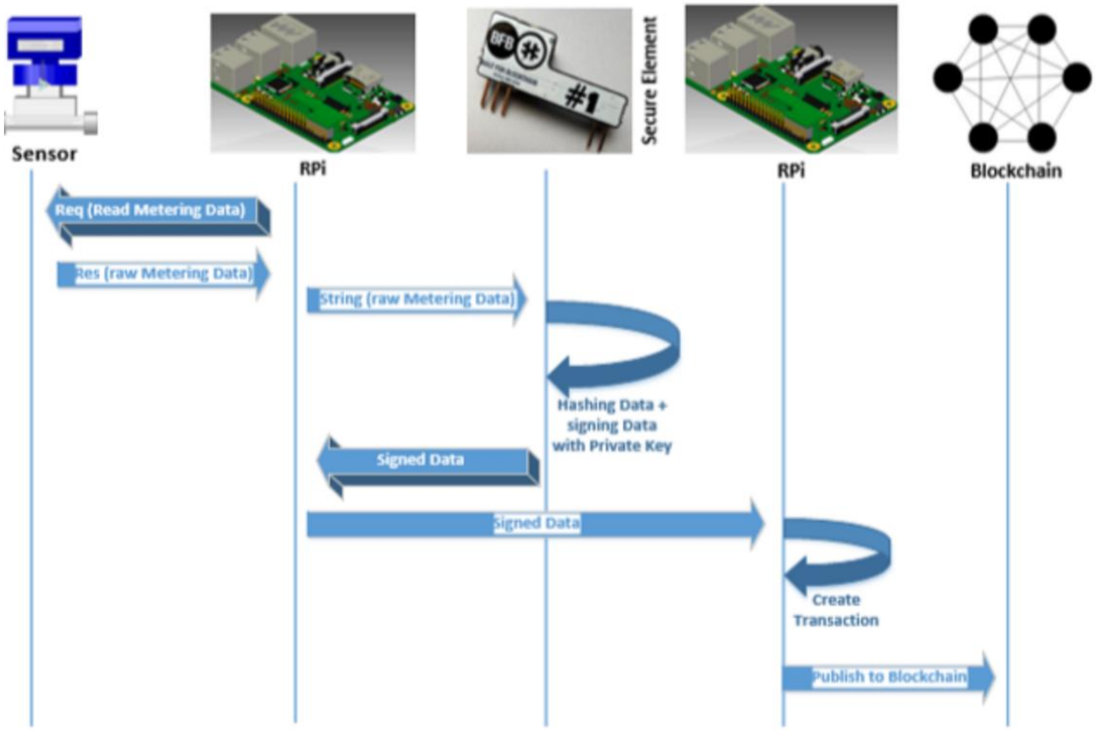


Figure 5-6: Data Flow Diagram

5. 7. 2 Experimental Setup and Tools Used

5. 7. 2. 1 BigchainDB Installation

BigchainDB is associated with some specific terminology, like BigchainDB client, node and network. For simulation test scenario we have built our private BigchainDB 2.2.2 that is minimum composed of 4 nodes. Each BigchainDB node (Figure 5-7) is composed of:

- MongoDB
- BigchainDB server
- Tendermint

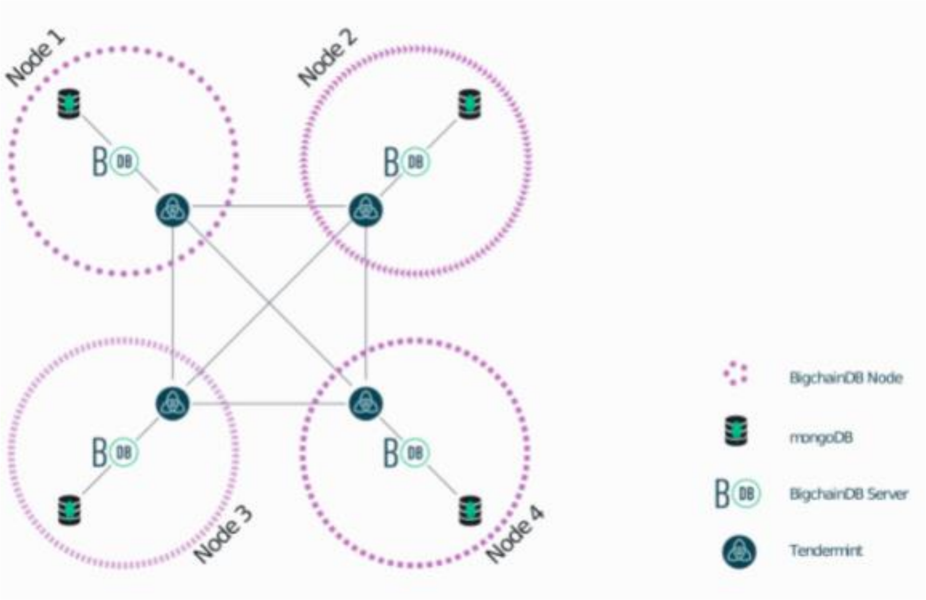


Figure 5-7: The four main components of BigchainDB network.

In BigchainDB starting version 2.0.0, each node has its own isolated local MongoDB database. The communication between nodes is done via Tendermint protocols and not MongoDB protocols, as presented in Figure 5-7. It is important to mention here that based on this database isolation, no other MongoDB databases (on other nodes) will be affected if a local MongoDB database node's is compromised.

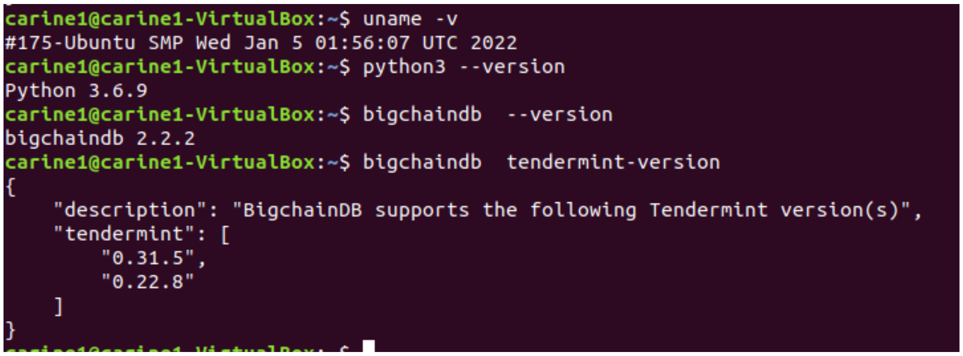
Our scenario implementation is based on using BigchainDB as database that is characterized by blockchain features. It has a high throughput, low latency and high performance it is decentralized and built-in asset support.

BigchainDB node environment setup:

Linux (UBUNTU) We used Linux (Ubuntu 18.04 and amd64 architecture) operating system for simple and fast setup. Since Linux is open source, it is very simple for anyone to solve some problems with Linux and there is a very good community that can support and help to solve any issues encountered. In our case, we have installed Ubuntu as it is convenient to handle and it is good for the decentralized network.

Python 3.6.9: for the setup and simulation phase, we have used PYTHON 3.6.9 version.

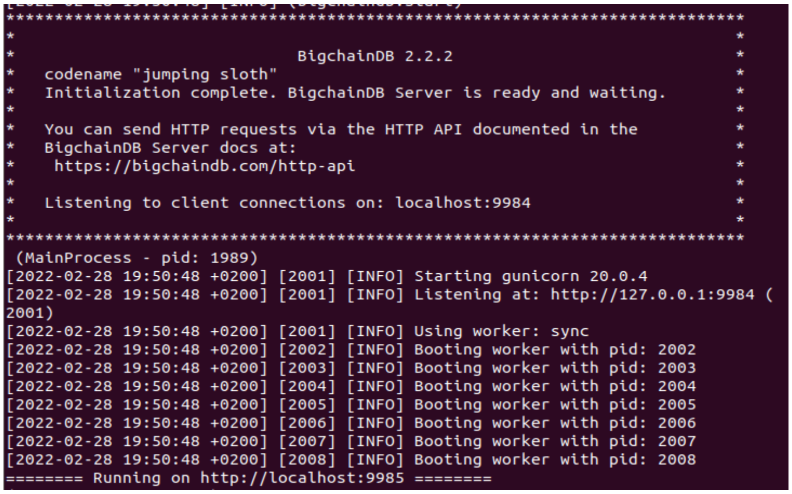
Figure 5-8 shows the different components version that are used to setup our testing environment.



```
carine1@carine1-VirtualBox:~$ uname -v
#175-Ubuntu SMP Wed Jan 5 01:56:07 UTC 2022
carine1@carine1-VirtualBox:~$ python3 --version
Python 3.6.9
carine1@carine1-VirtualBox:~$ bigchaindb  --version
bigchaindb 2.2.2
carine1@carine1-VirtualBox:~$ bigchaindb  tendermint-version
{
    "description": "BigchainDB supports the following Tendermint version(s)",
    "tendermint": [
        "0.31.5",
        "0.22.8"
    ]
}
carine1@carine1-VirtualBox:~$ 
```

Figure 5-8: Different System Versions.

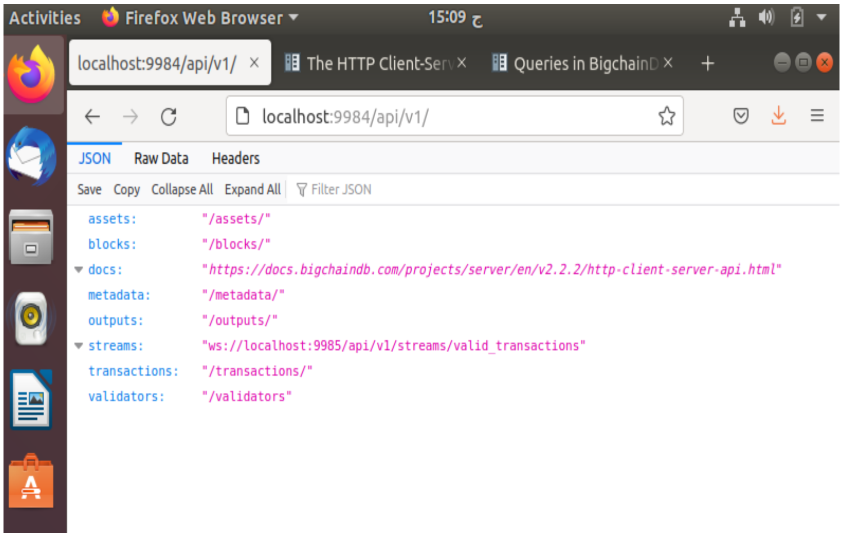
We have used Bigchaindb version 2.2.2 using pip3 and docker for installation. To run a BigchianDB sever (Figure 5-9) we have to install from GitHub repository Python library and packages and execute a docker functions or we can do a normal installation by using Python pip3. Figure 5-9 shows the BigchainDB server activation.



```
[2022-02-28 19:50:48] [INFO] (bigchaindb.start)
****************************************************************************
*                                                                          *
*                              BigchainDB 2.2.2                            *
*   codename "jumping sloth"                                               *
*   Initialization complete. BigchainDB Server is ready and waiting.       *
*                                                                          *
*   You can send HTTP requests via the HTTP API documented in the          *
*   BigchainDB Server docs at:                                             *
*    https://bigchaindb.com/http-api                                       *
*                                                                          *
*   Listening to client connections on: localhost:9984                     *
*                                                                          *
****************************************************************************
 (MainProcess - pid: 1989)
[2022-02-28 19:50:48 +0200] [2001] [INFO] Starting gunicorn 20.0.4
[2022-02-28 19:50:48 +0200] [2001] [INFO] Listening at: http://127.0.0.1:9984 (
2001)
[2022-02-28 19:50:48 +0200] [2001] [INFO] Using worker: sync
[2022-02-28 19:50:48 +0200] [2002] [INFO] Booting worker with pid: 2002
[2022-02-28 19:50:48 +0200] [2003] [INFO] Booting worker with pid: 2003
[2022-02-28 19:50:48 +0200] [2004] [INFO] Booting worker with pid: 2004
[2022-02-28 19:50:48 +0200] [2005] [INFO] Booting worker with pid: 2005
[2022-02-28 19:50:48 +0200] [2006] [INFO] Booting worker with pid: 2006
[2022-02-28 19:50:48 +0200] [2007] [INFO] Booting worker with pid: 2007
[2022-02-28 19:50:48 +0200] [2008] [INFO] Booting worker with pid: 2008
======== Running on http://localhost:9985 ========
```

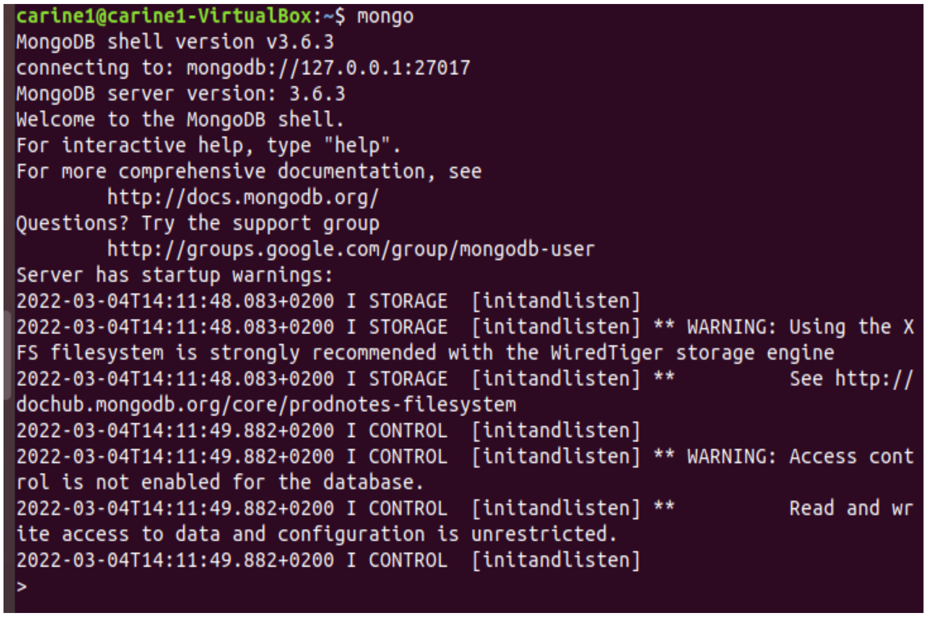
Figure 5-9: BigchainDB Server Activation

The data structure is the most specific thing to check and understand about BigchainDB. Contrary to how data is structured in conventional SQL database (like table) and in other non SQL database (like JSON) with BigchainDB data is represented as assets. Any kind of data it is either physical or object it is considered as an asset. Once the node is up and running a client can connect to the MongoDB either via BigchainDB API presented in ***Figure 5-10*** or via Shell presented in Figure 5-11. Also Compass which is a free GUI interface, can be used as a tool to interact with your MongoDB. Compass is an interactive free tool to query, optimize and analyze our MongoDB data (presented in Figure 5-12).



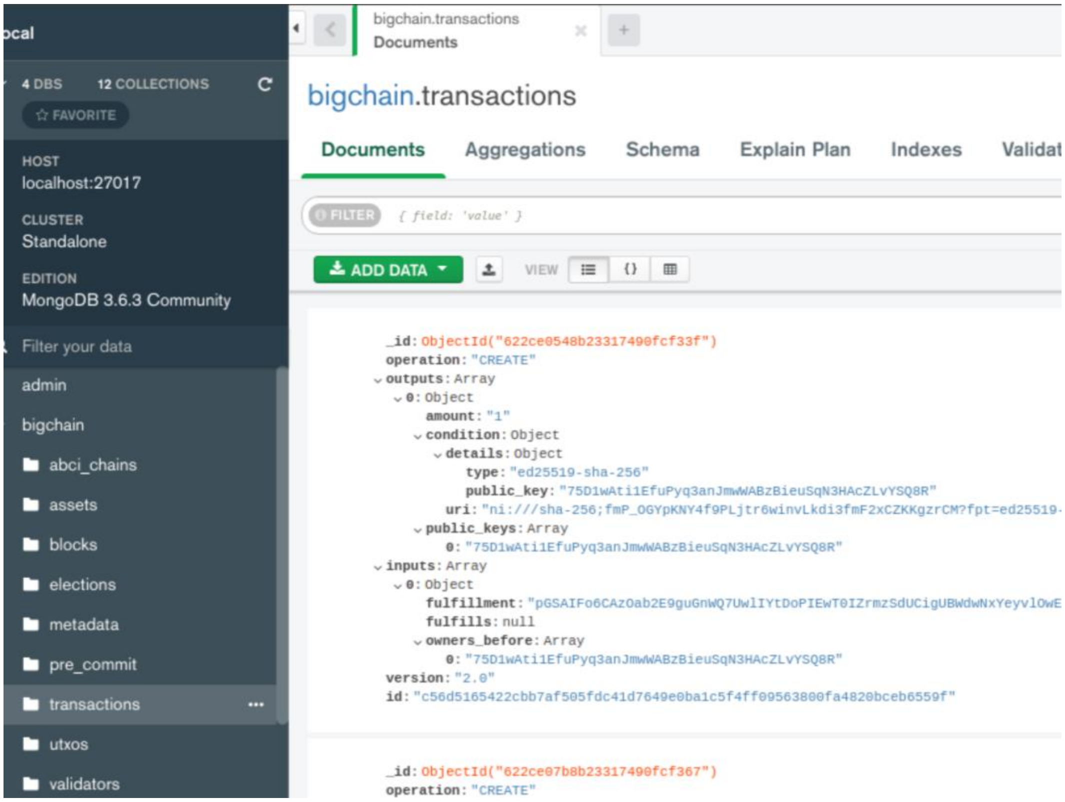
```
assets:        "/assets/"
blocks:        "/blocks/"
docs:          "https://docs.bigchaindb.com/projects/server/en/v2.2.2/http-client-server-api.html"
metadata:      "/metadata/"
outputs:       "/outputs/"
streams:       "ws://localhost:9985/api/v1/streams/valid_transactions"
transactions:  "/transactions/"
validators:    "/validators"
```

Figure 5-10: Connect to MongoDB via API



```
carine1@carine1-VirtualBox:~$ mongo
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27017
MongoDB server version: 3.6.3
Welcome to the MongoDB shell.
For interactive help, type "help".
For more comprehensive documentation, see
        http://docs.mongodb.org/
Questions? Try the support group
        http://groups.google.com/group/mongodb-user
Server has startup warnings:
2022-03-04T14:11:48.083+0200 I STORAGE  [initandlisten]
2022-03-04T14:11:48.083+0200 I STORAGE  [initandlisten] ** WARNING: Using the X
FS filesystem is strongly recommended with the WiredTiger storage engine
2022-03-04T14:11:48.083+0200 I STORAGE  [initandlisten] **          See http://
dochub.mongodb.org/core/prodnotes-filesystem
2022-03-04T14:11:49.882+0200 I CONTROL  [initandlisten]
2022-03-04T14:11:49.882+0200 I CONTROL  [initandlisten] ** WARNING: Access cont
rol is not enabled for the database.
2022-03-04T14:11:49.882+0200 I CONTROL  [initandlisten] **          Read and wr
ite access to data and configuration is unrestricted.
2022-03-04T14:11:49.882+0200 I CONTROL  [initandlisten]
>
```

Figure 5-11: Connect to MongoDB via Shell



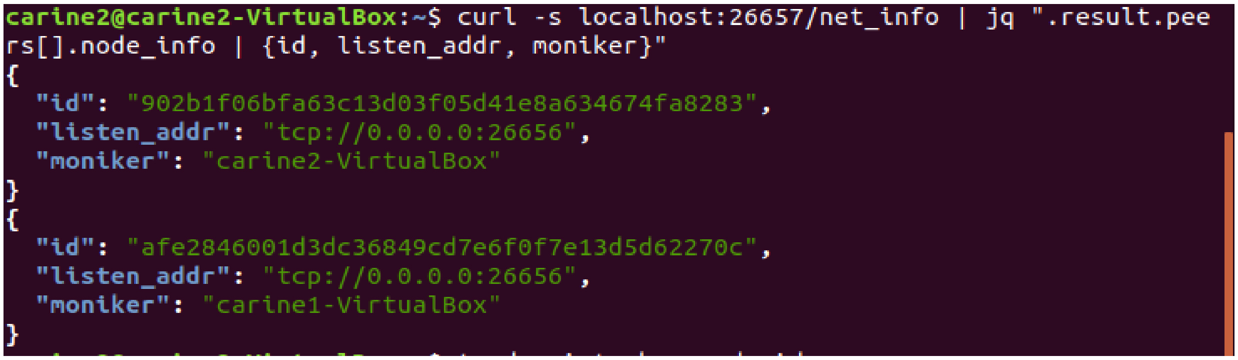
```
  _id: ObjectId("622ce0548b23317490fcf33f")
  operation: "CREATE"
⌄ outputs: Array
  ⌄ 0: Object
      amount: "1"
    ⌄ condition: Object
      ⌄ details: Object
          type: "ed25519-sha-256"
          public_key: "75D1wAti1EfuPyq3anJmwWABzBieuSqN3HAcZLvYSQ8R"
        uri: "ni:///sha-256;fmP_OGYpKNY4f9PLjtr6winvLkdi3fmF2xCZKKgzrCM?fpt=ed25519-
    ⌄ public_keys: Array
        0: "75D1wAti1EfuPyq3anJmwWABzBieuSqN3HAcZLvYSQ8R"
⌄ inputs: Array
  ⌄ 0: Object
      fulfillment: "pGSAIFo6CAzOab2E9guGnWQ7UwlIYtDoPIEwT0IZrmzSdUCigUBWdwNxYeyvlOwE
      fulfills: null
    ⌄ owners_before: Array
        0: "75D1wAti1EfuPyq3anJmwWABzBieuSqN3HAcZLvYSQ8R"
  version: "2.0"
  id: "c56d5165422cbb7af505fdc41d7649e0ba1c5f4ff09563800fa4820bceb6559f"

  _id: ObjectId("622ce07b8b23317490fcf367")
  operation: "CREATE"
```

Figure 5-12: Interact with MongoDB via Compass

As we have already mentioned the communication between nodes is done by Tendermint protocols.

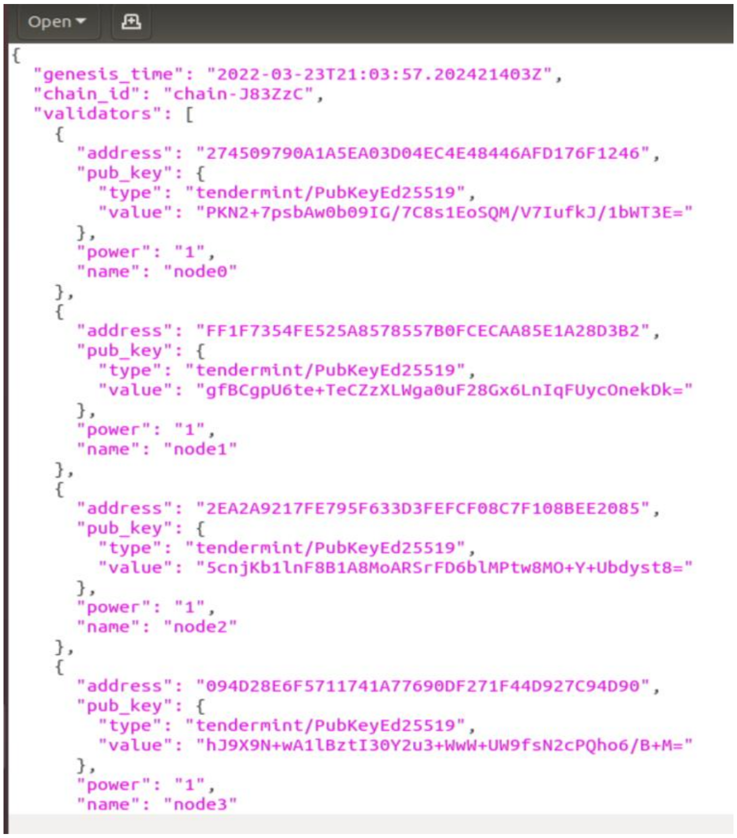
Tendermint which is a software that is used to replicate an application on many machines in a secure and consistent way, we mean by secure is that Tendermint works even if up to 1/3 of nodes fail in arbitrary ways and we mean by consistent that each non-faulty node sees the exact same transaction logs and computes the same state. One of the main problems of the distributed system is to ensure a secure and consistent replication, because it has a critical role in the fault tolerance for a wide range of applications like currencies and elections. Tendermint installation is one of the node BigchainDB setup steps. It is used to establish the communication between nodes. Once the Tendermint is installed it is enabled by using the below command "tendermint init", this command will create the required file for a single local node. In our case we had to create a cluster of four nodes therefore we have used the "tendermint testnet" command to create four directories of configuration files and we have copied each directory to the relevant node. Each node on the network is identified by its IP address. Four nodes should share the same genesis.json (Figure

5-14) file in order to establish a network (Figure 5-13). Note that after the third node is started, blocks will start to stream in because more then2/3 of validators have come online.



```
carine2@carine2-VirtualBox:~$ curl -s localhost:26657/net_info | jq ".result.pee
rs[].node_info | {id, listen_addr, moniker}"
{
  "id": "902b1f06bfa63c13d03f05d41e8a634674fa8283",
  "listen_addr": "tcp://0.0.0.0:26656",
  "moniker": "carine2-VirtualBox"
}
{
  "id": "afe2846001d3dc36849cd7e6f0f7e13d5d62270c",
  "listen_addr": "tcp://0.0.0.0:26656",
  "moniker": "carine1-VirtualBox"
}
```

Figure 5-13: List of Connected Nodes



```
{
  "genesis_time": "2022-03-23T21:03:57.202421403Z",
  "chain_id": "chain-J83ZzC",
  "validators": [
    {
      "address": "274509790A1A5EA03D04EC4E48446AFD176F1246",
      "pub_key": {
        "type": "tendermint/PubKeyEd25519",
        "value": "PKN2+7psbAw0b09IG/7C8s1EoSQM/V7IufkJ/1bWT3E="
      },
      "power": "1",
      "name": "node0"
    },
    {
      "address": "FF1F7354FE525A8578557B0FCECAA85E1A28D3B2",
      "pub_key": {
        "type": "tendermint/PubKeyEd25519",
        "value": "gfBCgpU6te+TeCZzXLWga0uF28Gx6LnIqFUycOnekDk="
      },
      "power": "1",
      "name": "node1"
    },
    {
      "address": "2EA2A9217FE795F633D3FEFCF08C7F108BEE2085",
      "pub_key": {
        "type": "tendermint/PubKeyEd25519",
        "value": "5cnjKb1lnF8B1A8MoARSrFD6blMPtw8MO+Y+Ubdyst8="
      },
      "power": "1",
      "name": "node2"
    },
    {
      "address": "094D28E6F5711741A77690DF271F44D927C94D90",
      "pub_key": {
        "type": "tendermint/PubKeyEd25519",
        "value": "hJ9X9N+wA1lBztI30Y2u3+WwW+UW9fsN2cPQho6/B+M="
      },
      "power": "1",
      "name": "node3"
```

Figure 5-14: Common genesis.json file

5. 7. 2. 2 Secure Element Setup

The Riddle & Code Secure Element was developed with dual targets, one to extend Arduino UNO R3 pin and two to extend all Raspberry Pi pin compliant boards, females' pins are used to connect the secure element to the RPi, however, male connectors are pins to be connected to Arduino UNO. Figure 5-15. Shows how the secure element is connected to our RPi.

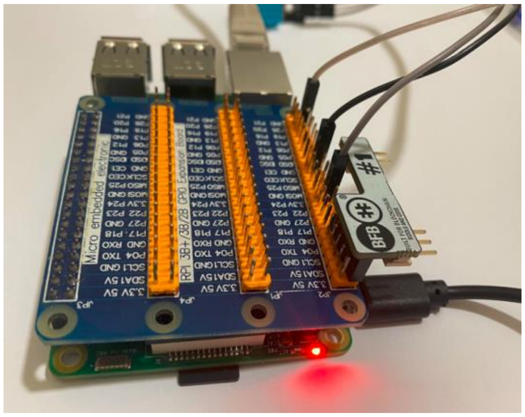


Figure 5-15: ***Hardware Connectivity***

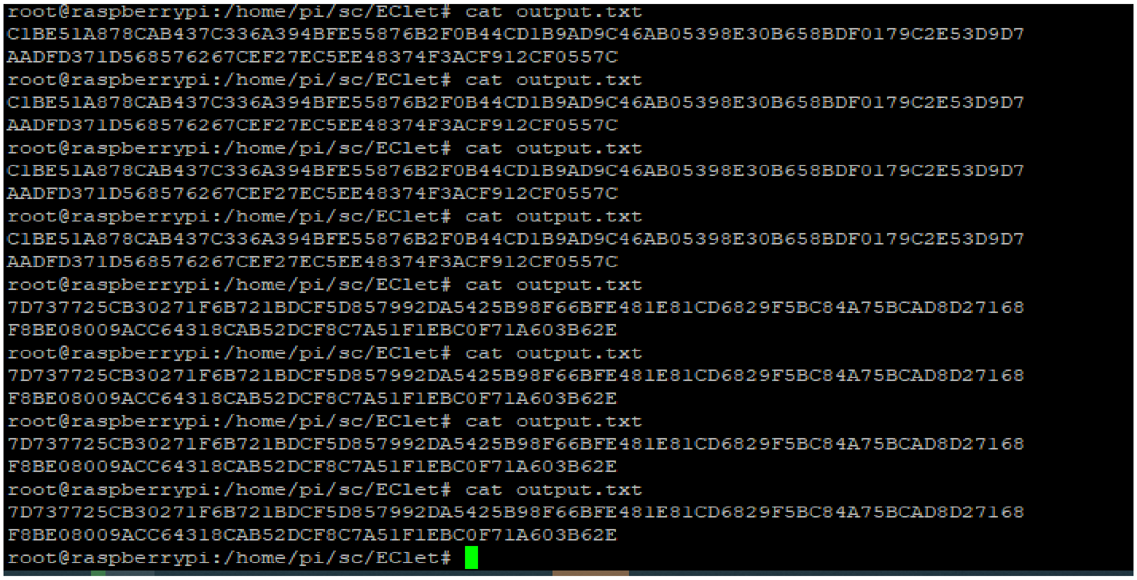
Once connected and configured the secure element on RPi, there is also a pre required environment that needs to be prepared. First, we should enable the communication between the SE and RPi via I2C and it should be configured as "Activate i2c via: raspi-config", in addition to the installation of some libraries like "libcryptoauth-0.2".

The I2C bus permits to different devices to be connected to our RPi, each device has a unique address that can often be configured by altering the jumper settings on the module. It is important to be able to identify which device is connected to our Pi just to make sure that everything is working properly.

5. 7. 3 Combinational Approach Testing & Results

The system is up and running and ready for testing after finalizing the hardware and software setup. The collected data from the sensor will be forwarded via the RPi to the secure element. At its turn the SE will encrypt and sign the data with a pair of generated keys at slot 0. B.

The secure element will return the encrypted and signed data to the RPi where it will in turn transmit that data to BigchainDB. Below is the secure element output:



```
root@raspberrypi:/home/pi/sc/EClet# cat output.txt
C1BE51A878CAB437C336A394BFE55876B2F0B44CD1B9AD9C46AB05398E30B658BDF0179C2E53D9D7
AADFD371D568576267CEF27EC5EE48374F3ACF912CF0557C
root@raspberrypi:/home/pi/sc/EClet# cat output.txt
C1BE51A878CAB437C336A394BFE55876B2F0B44CD1B9AD9C46AB05398E30B658BDF0179C2E53D9D7
AADFD371D568576267CEF27EC5EE48374F3ACF912CF0557C
root@raspberrypi:/home/pi/sc/EClet# cat output.txt
C1BE51A878CAB437C336A394BFE55876B2F0B44CD1B9AD9C46AB05398E30B658BDF0179C2E53D9D7
AADFD371D568576267CEF27EC5EE48374F3ACF912CF0557C
root@raspberrypi:/home/pi/sc/EClet# cat output.txt
C1BE51A878CAB437C336A394BFE55876B2F0B44CD1B9AD9C46AB05398E30B658BDF0179C2E53D9D7
AADFD371D568576267CEF27EC5EE48374F3ACF912CF0557C
root@raspberrypi:/home/pi/sc/EClet# cat output.txt
7D737725CB30271F6B721BDCF5D857992DA5425B98F66BFE481E81CD6829F5BC84A75BCAD8D27168
F8BE08009ACC64318CAB52DCF8C7A51F1EBC0F71A603B62E
root@raspberrypi:/home/pi/sc/EClet# cat output.txt
7D737725CB30271F6B721BDCF5D857992DA5425B98F66BFE481E81CD6829F5BC84A75BCAD8D27168
F8BE08009ACC64318CAB52DCF8C7A51F1EBC0F71A603B62E
root@raspberrypi:/home/pi/sc/EClet# cat output.txt
7D737725CB30271F6B721BDCF5D857992DA5425B98F66BFE481E81CD6829F5BC84A75BCAD8D27168
F8BE08009ACC64318CAB52DCF8C7A51F1EBC0F71A603B62E
root@raspberrypi:/home/pi/sc/EClet# cat output.txt
7D737725CB30271F6B721BDCF5D857992DA5425B98F66BFE481E81CD6829F5BC84A75BCAD8D27168
F8BE08009ACC64318CAB52DCF8C7A51F1EBC0F71A603B62E
root@raspberrypi:/home/pi/sc/EClet# 
```

Figure 5-16: Secure Element Output

Transaction in BigchainDB: in BigchainDB, transaction is usually used to register, issue, create and transfer data (called assets). An asset can be any physical object like bike, car or digital asset like a customer object. In a transaction, the assets are immutable and each asset can have a metadata that is mutable and updated in the next transactions. Transactions have an input and output and are the basic type of records stored by BigchainDB. Actually there are two type of transactions: CREATE and TRANSFER.

CREATE Transactions: the create transaction function is used to create, issue and register an asset it is the history of an asset in BigchainDB. A create transaction has one or more outputs. Every output has an associated number of shares. For example, if 50 oak trees is associated to an asset, one output may have 35 oak trees for a group of owners and the second output may have 15 oak trees for the second group of owners. Every output has also an associated condition: conditions must be full filed by transfer transaction to transfer the output. BigchainDB has different variety of conditions.

Figure 5-17: ***BigchainDB CREATE Transaction***

In Figure 5-17 we see a diagram that presents a BigchainDB CREATE transaction, that has one output which is Pam that owns and controls 3 shares of the assets and there no other shares since there are no more outputs.

A TRANSFER transaction: transfers ownership of an asset, by providing an input that meets the conditions of an earlier transaction's outputs. With a transfer transaction you can have one or more outputs just like the create transaction. And the total number of shares coming in on the inputs must be equal to the number of share going out on the outputs.

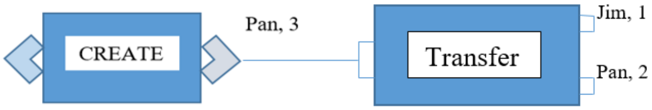


Figure 5-18: BigchainDB Transfer Transaction

Let's consider the creation and transfer of a digital asset between two neighbors (A and B). This asset represents the extra available energy metering data. We'll suppose that the extra energy data belongs to neighbor A, and that it will be transferred to neighbor B (knowing that is data is the output of the secure element presented in Figure 5-16. In order to create a transaction, neighbor A has to define the asset and then create a transaction.

Asset definition:

```
energy = {
    'data': {
        'energy': {
            'amount': 'secure element output',
            'unit': 'kWh',
        },
    },
```

}

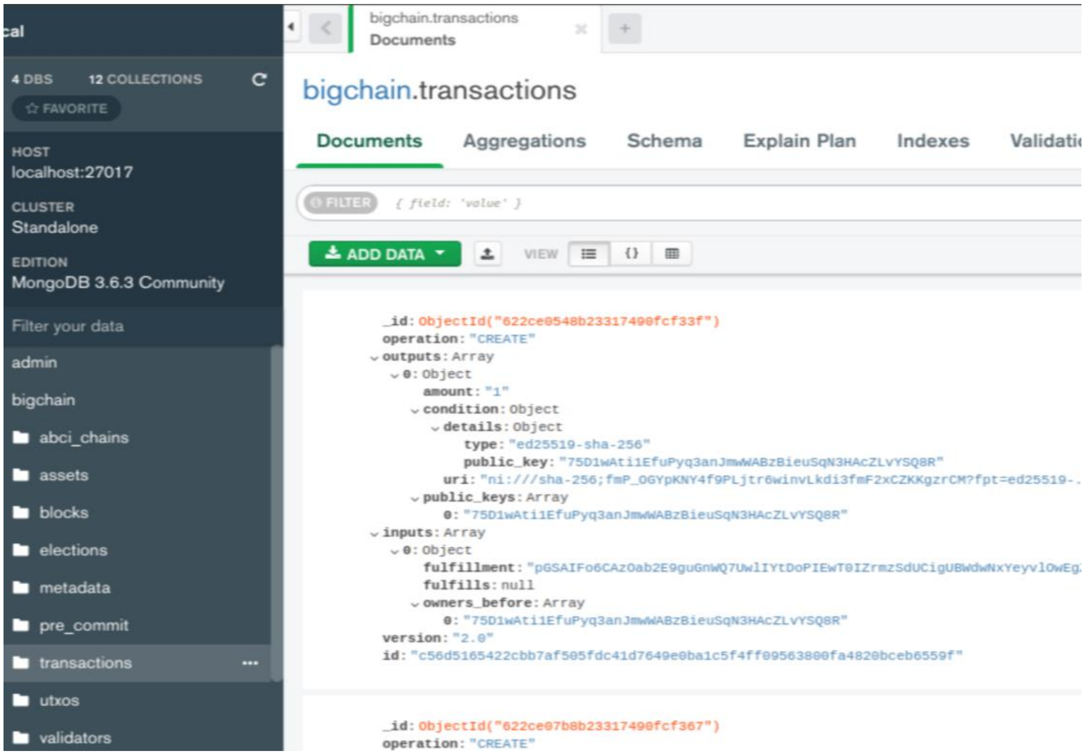
BigchainDB users are identified by public/private key pairs. The private key is used to sign transactions, while the public key is used to verify that a signed transaction was truly signed by the one who claims to be the signer. Now neighbor A is ready to create the asset (Figure 5-19).

<u>Asset creation:</u>

```
prepared_creation_tx = bdb.transactions.prepare(
   operation='CREATE',
   signers=neighborA.public_key,
   asset=energy,
   )
```

Now the transaction has to be fulfilled by signing it with neighbor A private key.

```
fulfilled_creation_tx = bdb.transactions.fulfill(
      prepared_creation_tx, private_keys=neighboreA.private_key)
```



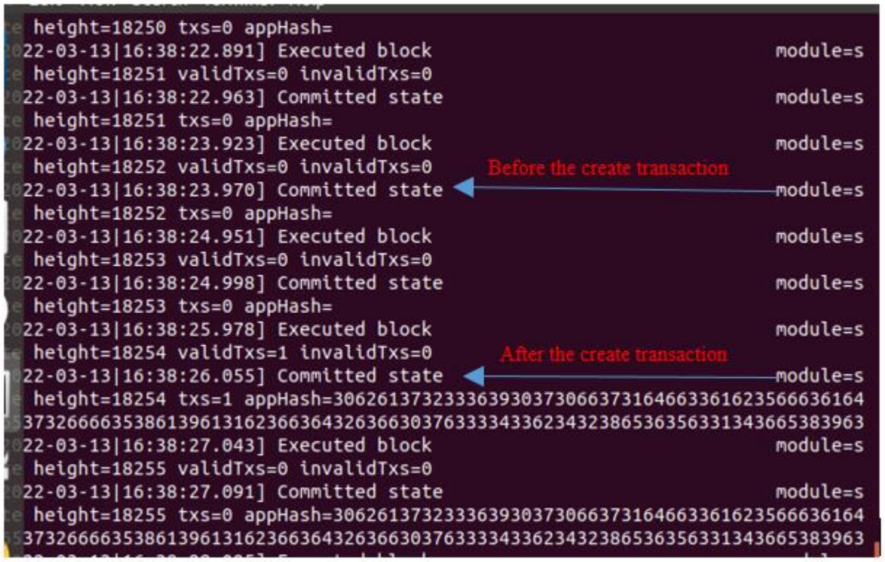
```
_id: ObjectId("622ce0548b23317490fcf33f")
operation: "CREATE"
outputs: Array
  0: Object
    amount: "1"
    condition: Object
      details: Object
        type: "ed25519-sha-256"
        public_key: "75D1wAti1EfuPyq3anJmwWABzBieuSqN3HAcZLvYSQ8R"
      uri: "ni:///sha-256;fmP_OGYpKNY4f9PLjtr6winvLkdi3fmF2xCZKKgzrCM?fpt=ed25519-.
    public_keys: Array
      0: "75D1wAti1EfuPyq3anJmwWABzBieuSqN3HAcZLvYSQ8R"
inputs: Array
  0: Object
    fulfillment: "pGSAIFo6CAzOab2E9guGnWQ7UwlIYtDoPIEwT0IZrmzSdUCigUBWdwNxYeyvlOwEg
    fulfills: null
    owners_before: Array
      0: "75D1wAti1EfuPyq3anJmwWABzBieuSqN3HAcZLvYSQ8R"
version: "2.0"
id: "c56d5165422cbb7af505fdc41d7649e0ba1c5f4ff09563800fa4820bceb6559f"

_id: ObjectId("622ce07b8b23317490fcf367")
operation: "CREATE"
```

Figure 5-19: ***Create Transaction***

Once the asset is created and signed by the owner, now it can be transferred to the BigchainDB node using the following function:

```
sent_creation_tx = bdb.transactions.send_commit(fulfilled_creation_tx)

sent_creation_tx == fulfilled_creation_tx

txid = fulfilled_creation_tx['id']
```

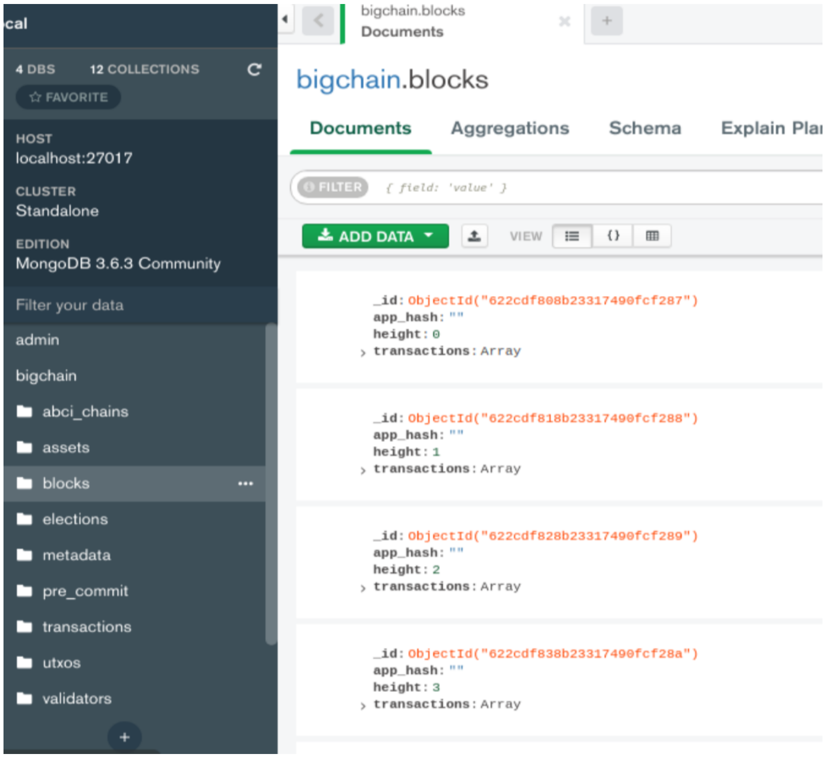
Usually after a few seconds of sending the transaction to the BigchainDB node, it is important to verify that the transaction was sent successfully, validated and included in a block. If the transaction succeed this will return the block height containing the transaction however, if it failed then no block generation and will get None as a return. There are different reasons behind the None for example it could be related to the validity of the transaction or to delay and the transaction will still be in the queue. Usually an exception is raised in case of invalid transaction. After running the creation code block creation starts as per Figure 5-20.



```
 height=18250 txs=0 appHash=
22-03-13|16:38:22.891] Executed block                                module=s
 height=18251 validTxs=0 invalidTxs=0
22-03-13|16:38:22.963] Committed state                               module=s
 height=18251 txs=0 appHash=
22-03-13|16:38:23.923] Executed block                                module=s
 height=18252 validTxs=0 invalidTxs=0
22-03-13|16:38:23.970] Committed state                               module=s
 height=18252 txs=0 appHash=
22-03-13|16:38:24.951] Executed block                                module=s
 height=18253 validTxs=0 invalidTxs=0
22-03-13|16:38:24.998] Committed state                               module=s
 height=18253 txs=0 appHash=
22-03-13|16:38:25.978] Executed block                                module=s
 height=18254 validTxs=1 invalidTxs=0
22-03-13|16:38:26.055] Committed state                               module=s
 height=18254 txs=1 appHash=306261373233363930373066373164663361623566636164
3732666635386139613162366364326366303763333433623432386536356331343665383963
22-03-13|16:38:27.043] Executed block                                module=s
 height=18255 validTxs=0 invalidTxs=0
22-03-13|16:38:27.091] Committed state                               module=s
 height=18255 txs=0 appHash=306261373233363930373066373164663361623566636164
3732666635386139613162366364326366303763333433623432386536356331343665383963
```

Figure 5-20: ***Block Creation***

To check the whole block we can use the block height to retrieve the block itself or also we use Mongo compact to interact easily with mongo DB as presented in Figure 5-21.



```
_id: ObjectId("622cdf808b23317490fcf287")
app_hash: ""
height: 0
› transactions: Array

_id: ObjectId("622cdf818b23317490fcf288")
app_hash: ""
height: 1
› transactions: Array

_id: ObjectId("622cdf828b23317490fcf289")
app_hash: ""
height: 2
› transactions: Array

_id: ObjectId("622cdf838b23317490fcf28a")
app_hash: ""
height: 3
› transactions: Array
```

***Figure 5-21:* Block Enablement**

After neighbor A successfully create the asset and submit to the blockchain it decided to transfer asset ownership to neighbor B. Neighbor A retrieve the transaction id "creation_tx = bdb.transactions.retrieve(txid)". In order to prepare the transfer transaction, neighbor A has to know the asset id using the below functions.

```
asset_id = creation_tx['id']


transfer_asset = {
  'id': asset_id,
}
```

Once the id is retrieve neighbor A can prepare the transfer transaction, fulfill it and finally send it to the connected BigchainDB node as below:

```
output_index = 0
```

```
output = creation_tx['outputs'][output_index]
transfer_input = {
    'fulfillment': output['condition']['details'],
    'fulfills': {
       'output_index': output_index,
       'transaction_id': creation_tx['id'],
     },
     'owners_before': output['public_keys'],
  }
prepared_transfer_tx = bdb.transactions.prepare(
    operation='TRANSFER',
    asset=transfer_asset,
    inputs=transfer_input,
   recipients=neighborB.public_key,
  )
  fulfilled_transfer_tx = bdb.transactions.fulfill(
     prepared_transfer_tx,
     private_keys=neighborA.private_key,
  )
sent_transfer_tx = bdb.transactions.send_commit(fulfilled_transfer_tx)
```

Now neighbor B is the owner of the asset and neighbor A is the former owner. Now neighbor B has access and owns the asset and is capable of decrypting the data through its secure element.

The feasibility of combining blockchain and Secure Element has been studied and argued about its advantages and demonstrated with the experimental implementation. The proposed prototype is tested using BigchainDB and Ridle&code secure element. The adoption of the above scenario allowed a secure data transmission between two clients and present a secure prototype for

IoT platform. The developed code permits the creation and transmission of energy data between two neighbors.

5. 8 Conclusion

In this chapter we have presented the combinational approach using blockchain and SE. We have implemented and tested this approach using a secure element in combination with blockchain. As a case study, we have applied our prototype to the energy field to allow a secure P2P energy trading.

We have started this chapter by introducing the characteristics of both blochchain and secure element technologies. Then we have described and explained how blockchain can be used as distribution data base for secure data storage and transactions. We have also mentioned that the implementation of the blockchain alone is insufficient to provide end to secure the IoT platform. If the data is modified before being stored on the bockchain, it will affect the consensus decision and will result in a conflict between the validators. Since blockchain can't penetrate to lower levels, here is the proposal to integrate secure element.

We have designed and tested a solution that uses Riddle & Code as a secure element and BigchainDB as a distributed data base. As a case study of the tested solution is the P2P energy trade where the IoT devices that we have worked on represent the SMGW. The SMGW is presented as a BigchainDB client that is capable to interact with BigchainDB to create an asset and register its data on the distributed data base. This tested model presents a secure version since we were able by the integration of secure element to encrypt the data at the source of generation and the decrypt at the destination or the new owner.

The main result of our experiments, is that based on these two technologies we were able to present an end-to-end secure system for energy trade. The integration of secure element at the node level provide IoT devices with some computational power and secure data at the point of generation and the use of a blockchain as a distributed data base is to overcome some security and trust challenges for IoT platforms.

General Conclusion & Perspectives

General Conclusion & Perspectives

In this thesis we have addressed the impediment faced by the integration of renewable energy resources (RES), maintaining the security of energy supply and encouraging the future energy market .As a result, the implementation of such a system requires a versatile communication platform to exchange data between legacy and new smart grid applications.

In chapter 1 we introduced the generalities concerning a detailed bibliographic study of a smart grid and the advanced metering infrastructure system. The bibliographic study is presented by evaluating the performance of the Advanced Metering Infrastructure (AMI) system and its communication technologies used to identify potential cyber security issues. the evolution of the conventional energy grid is achieved by defining and describing the Advanced Metering Infrastructure (AMI) system. We discussed the communication technologies in use, in addition to a quick bibliographical study that covers the cyber security vulnerabilities of smart metering based on LPWAN wireless communication technologies, where we showed some security breaches related to the SG system, can compromise the entire system and threaten user's privacy. Therefore, we have developed some AMI security best practices that can secure the system, listed at the end.

Following that in Chapter 2 we presented an overview of the current and future developments in IoE, use cases, applications and related plans of action in Europe were provided. A particular focus, on introducing IoE current state in Europe countries like Germany and Greece. The German system was presented and discussed in detail since it was used as a reference architecture of our developed energy metering gateway.

Next after the bibliographical study, the following chapters 3 and 4 present the conception, the realization of an open-source energy gateway, and the overcome constraint and challenges that we faced in terms of design, and modularity. The prototype designed has been detailed, in addition, the implementation and testing results were explained and discussed. Both chapters propose the design and deployment of an open-source, low-cost, and modular system based on LoRa telecommunication technology for energy metering applications.

Specifically in chapter 3, we presented the solution that was designed and proposed for the Lebanese market as an important solution to access the electricity outages by deploying a near real-time energy metering infrastructure. The design was deployed and tested in an experimental energy metering application, where the measured values have been published on a cloud server, allowing to run analytics and be accessible by the Energy sector operators and the smart meter owners simultaneously. These values can be accessed, processed, and presented using a multitude set of tools enabling the deployment of third-party valuable services like the implementation of Virtual Power Plants for Energy curtailment, and the introduction of Distributed Ledger Technologies for peer-to-peer energy trading.

In Chapter 4 we presented the benefits of adopting low-cost IoT solutions and Smart Metering communication protocol standards targeting the renovation of existing electricity Grids to Smart Grids with peer-to-peer electricity exchange capabilities. Towards this scope, we propose a Smart Grid Architecture based on the DLMS/COSEM energy-metering communication standard and LPWAN communication technologies, while a Blockchain layer enables the smart-metering data integrity for electricity trading.

The final chapter going a step further we examined and tested the implementation of an SMGW based blockchain and secure element, such as enabling technology for energy digitization. To provide an end to end secure P2P energy trading system, the introduction of Blockchain (BC) alone, which is a new paradigm with the potential to overcome security and trust challenges for IoT platforms, as a distributed data base partially solves the issue. Blockchain alone by itself is not able to completely secure a transaction because it is only guarantee data immutability while in most cases the data has to be secured at the point of generation. Furthermore, due to its significant overhead blockchain is not able to penetrate to lower levels in a system. Therefore, to fill this gap this chapter proposed the use of Secure Elements (SE) to build a "root of trust", and to provide IoT devices trusted computing resources to generate a cryptographic signature, following the secure by design model. The combination of these two technologies helps to overcome the obstructions of using just one technology alone. This new approach was used as base of our suggested end-to-end secure and decentralized IoT system that was applied and tested in energy smart metering gateway to enable local P2P energy trading.

Based on the experimental tests, we have presented a secure open-source end to end system for energy trading, where the integration of secure elements at the node level provides IoT devices with some computational power and secure data at the point of generation and the use of a blockchain as a distributed data base to overcome some security and trust challenges for IoT platforms. The open-source smart meter gateway presented by this work provides a secure end to end trading system.

This thesis work can be considered as a contribution in providing an open-source smart meter gateway, which combines different new technologies to present a secure end to end solution for P2P energy trading. This system integrates IoT, blockchain, secure element and LPWAN all technologies together to find a solution that secures the data from source of generation to destination. We believe that with this approach presented in this thesis, even more roles can be played by this developed gateway while many of the existing functionalities could be further improved. We suggest few as follows:

- Short Term:
   - ➢ Different brands of secure element combined with different blockchain could be implemented and tested to present different aspects of the solution and to compare different vendors. This work is almost done and an article will be published soon.
   - ➢ Later a comparative analysis on usage of virtual SE instead of a hard SE for blockchain application, where a virtual SE is a secure sandbox that is embedded within the operating system which creates a secure and safe environment similar to SE.
- **Medium Term : Application of this approach**
   - ➢ This will include installation of this system in a number of residential and small commercial settings, where more detailed tests of the ability of our SMGW to work in different neighborhood area network setups and in different environments will be tested.
   - ➢ Future tests also proposed to improve and develop this tested open source smart meter gateway to be integrated in smart grid system.
- **Long Term**

- This combinational approach SE and Blockchain can be used and adopted as the basis for P2P trading platforms. Independently of the asset that we are trading.
- Future research is also needed to evaluate the use of SMGW in the use cases presented below:
  - Smart city optimization, this is by connecting physical object to blockchain. When physical nodes can communicate securely within a distributed environment it enables smart city optimization.
  - Tests will be contemplated to examine our SMGW capabilities to record energy use and storage data related to electric vehicle charging
- Rolling out the energy solution and improving this product for the new era of distributed energy that empowers utility providers to bring trust and flexibility towards local energy communities, to enable the production of renewable energy and to prepare for the token economy to come.

References

Chapter 1 References:

[1] "Smart Energy." Smart Energy International, 19 July 2018, www.smart-energy.com/regional-news/north-america/russia-attacked-the-us-power-grid-what-if-they-dont-stop. (accessed on Juin 2020)

[2] "Smart Energy." Smart Energy International, 23 July 2019, www.smart-energy.com/industry-sectors/smart-meters/just-153-3-million-lpwan-smart-meters-from-2019-2028. (accessed on Juin 2020)

[3] W. Liu, J. Zhan, and C. Y. Chung, "Transactions on Power Systems A Novel Transactive Energy Control Mechanism for Collaborative Networked Microgrids," IEEE Trans. Power Syst., vol. PP, no. c, p. 1, 2018, doi: 10.1109/TPWRS.2018.2881251.

[4] "Applying Blockchain Technology to Electric Power Systems." Smart Energy International, 31 Oct. 2018, www.smart-energy.com/industry-sectors/policy-regulation/applying-blockchain-technology-electric-power-systems. (accessed on Juin 2020)

[5] J. A. P. Lopes, N. Hatziargyriou, J. Mutale, P. Djapic, and N. Jenkins, "Integrating distributed generation into electric power systems: A review of drivers, challenges and opportunities," Electr. Power Syst. Res., vol. 77, no. 9, pp. 1189–1203, 2007, doi: 10.1016/j.epsr.2006.08.016.

[6] "Iea." Renewables 2017, Oct. 2018, www.smart-energy.com/industry-sectors/policy-regulation/applying-blockchain-technology-electric-power-systems. (accessed on Juin 2020)

[7] H. Hooshyar and L. Vanfretti, "A SGAM-based architecture for synchrophasor applications facilitating TSO/DSO interactions," 2017 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. ISGT 2017, no. April, 2017, doi: 10.1109/ISGT.2017.8085977.

[8] Bruinenberg, J.; Colton, L.; Darmois, E.; Dorn, J.; Doyle, J.; Elloumi, O.; Englert, H.; Forbes, R.; Heiles, J.; Hermans, P.; et al. CEN-CENELEC-ETSI: Smart Grid Coordination Group—Smart Grid Reference Architecture Report 2.0. 2012, https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf (accessed on 30 December 2020)

[9] N. Uribe-Pérez, L. Hernández, D. de la Vega, and I. Angulo, "State of the Art and Trends Review of Smart Metering in Electricity Grids," Appl. Sci., vol. 6, no. 3, pp. 1–24, 2016, doi: 10.3390/app6030068.

[10] G. Barnicoat and M. Danson, "The ageing population and smart metering: A field study of householders' attitudes and behaviours towards energy use in Scotland," Energy Res. Soc. Sci., vol. 9, pp. 107–115, 2015, doi: 10.1016/j.erss.2015.08.020.

[11] Farhangi, H. "The Path of the Smart Grid." IEEE Power and Energy Magazine, vol. 8, no. 1, Institute of Electrical and Electronics Engineers (IEEE), Jan. 2010, pp. 18–28. Crossref, https://doi.org/10.1109/mpe.2009.934876..

[12] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," IEEE Commun. Surv. Tutorials, vol. 15, no. 1, pp. 5–20, 2013, doi: 10.1109/SURV.2012.021312.00034.

[13] “Smart Meters and Smart Meter Systems : A Metering Industry Perspective” no. March, 2011.

[14] M. R. Abid, A. Khallaayoun, H. Harroud, R. Lghoul, M. Boulmalf, and D. Benhaddou, “A wireless mesh architecture for the advanced metering infrastructure in residential smart grids,” IEEE Green Technol. Conf., pp. 338–344, 2013, doi: 10.1109/GreenTech.2013.58.

[15] F. Halim, S. Yussof, and M. E. Rusli, “Cyber Security Issues in Smart Meter and Their Solutions,” Int. J. Comput. Sci. Netw. Secur, vol. 18, no. 3, pp. 99–109, 2018.

[16] P. W. Schultz, M. Estrada, J. Schmitt, R. Sokoloski, and N. Silva-Send, “Using in-home displays to provide smart meter feedback about household electricity consumption: A randomized control trial comparing kilowatts, cost, and social norms,” Energy, vol. 90, pp. 351–358, 2015, doi: 10.1016/j.energy.2015.06.130.

[17] F. Molazem, “Security and Privacy of Smart Meters : A Survey,” Work. Pap, pp. 1–11, 2012,[Online].Available:http://blogs.ubc.ca/computersecurity/files/2012/04/FMolazem_SurveyFaridMolazem.pdf.

[18] “Networked energy services,” ANSI Smart Meter.: https://www.networkedenergy.com/en/products/ANSI-smart-meter (accessed Sep. 15, 2019).

[19] “Networked energy services,” IEC Single Phase Smart Meter Device. https://www.networkedenergy.com/en/products/iec-single-phase-meter (accessed Sep. 15, 2019).

[20] S. Shekara, S. Reddy, L. Wang, and V. Devabhaktuni, “Smart meters for power grid : Challenges, issues, advantages and status,” Renew. Sustain. Energy Rev., vol. 15, no. 6, pp. 2736–2742, 2011, doi: 10.1016/j.rser.2011.02.039.

[21] R. Rashed Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar, “A survey on Advanced Metering Infrastructure,” Int. J. Electr. Power Energy Syst., vol. 63, pp. 473–484, 2014, doi: 10.1016/j.ijepes.2014.06.025.

[22] A. A. Khan, M. H. Rehmani, and M. Reisslein, “Cognitive Radio for Smart Grids : Survey of Architectures, Spectrum Sensing Mechanisms, and Networking Protocols,” no. c, pp. 1–41, 2015, doi: 10.1109/COMST.2015.2481722.

[23] H. Hu, D. Kaleshi, A. Doufexi, and L. Li, “Performance analysis of IEEE 802.11af standard based neighborhood area network for smart grid applications,” IEEE Veh. Technol. Conf., vol. 2015, pp. 0–4, 2015, doi: 10.1109/VTCSpring.2015.7146000.

[24] T. Chen, “Smart grids, smart cities need better networks,” IEEE Netw., vol. 24, no. 2, pp. 2–3, 2010, doi: 10.1109/MNET.2010.5430136.

[25] C. Gomez and J. Paradells, “Survey of home automation networks,” IEEE Commun. Mag., no. June, pp. 92–101, 2010, [Online]. Available: http://www.ann.ece.ufl.edu/courses/eel6935_11fal/papers/Survey of home automation networks.pdf.

[26] S. Khanji, F. Iqbal, and P. Hung, “ZigBee Security Vulnerabilities: Exploration and Evaluating,” 2019 10th Int. Conf. Inf. Commun. Syst. ICICS 2019, no. July, pp. 52–57, 2019, doi: 10.1109/IACS.2019.8809115.

[27] N. Vidgren, K. Haataja, J. L. Patiño-Andres, J. J. Ramírez-Sanchis, and P. Toivanen, “Security threats in ZigBee-enabled systems: Vulnerability evaluation, practical experiments, countermeasures, and lessons learned,” Proc. Annu. Hawaii Int. Conf. Syst. Sci., pp. 5132–5138, 2013, doi: 10.1109/HICSS.2013.475.

[28] S. Marksteiner, V. J. E. Jimenez, H. Valiant, and H. Zeiner, “An overview of wireless IoT protocol security in the smart home domain,” Jt. 13th CTTE 10th C. Conf. Internet Things - Bus. Model. Users, Networks, vol. 2018-Janua, pp. 1–8, 2017, doi: 10.1109/CTTE.2017.8260940.

[29] Z. Alliance, “ZigBee Specificarion,” Stand. Oct, 2015, [Online]. Available: http://ieeexplore.ieee.org/document/6264290/.

[30] Cryptographic Mechanisms: Recommendations and Key Lengths,” BSI – Technical Guideline,Jan.2022.https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=10. (accessed May 15, 2022).

[31] B. Fouladi and S. Ghanoun, “Security Evaluation of the Z-Wave Wireless Protocol,” Black hat, p. 6, 2013.

[32] B. M. Dörge and T. Scheffler, “Using IPv6 and 6LoWPAN for home automation networks,” Dig. Tech. Pap. - IEEE Int. Conf. Consum. Electron. pp. 44–47, 2011, doi: 10.1109/ICCE-Berlin.2011.6031865.

[33] K. F. Tsang, W. C. Lee, K. L. Lam, H. Y. Tung, and K. Xuan, “An integrated ZigBee automation system: An energy saving solution,” Proc. 14th Int. Conf. Mechatronics Mach. Vis. Pract. M2VIP2007, pp. 252–258, 2007, doi: 10.1109/MMVIP.2007.4430752.

[34] J. S. Lee, C. C. Chuang, and C. C. Shen, “Applications of short-range wireless technologies to industrial automation: A zigbee approach,” Proc. 2009 5th Adv. Int. Conf. Telecommun. AICT 2009, pp. 15–20, 2009, doi: 10.1109/AICT.2009.9.

[35] “Semtech,” Smart Homes. https://www.semtech.com/lora/lora-applications/smart-homes (accessed Sep. 15, 2021).

[36] S. Ravi, Deciphering Natural Language. Proquest, UMI Dissertation Publishing, 2012.

[37] V. Mohan, “An introduction to wireless M-Bus,” Silicon Labs, 2015, [Online]. Available: http://pages.silabs.com/rs/634-SLU-379/images/introduction-to-wireless-mbus.pdf.

[38] Boulogeorgos, P. D. Diamantoulakis, and G. K. Karagiannidis, “Low power wide area networks (lpwans) for internet of things (iot) applications: Research challenges and future trends,” arXiv preprint arXiv:1611.07449, 2016.

[39] L. Germani, V. Mecarelli, G. Baruffa, L. Rugini, and F. Frescura, “An IoT architecture for continuous livestock monitoring using lora LPWAN,” Electron., vol. 8, no. 12, 2019, doi: 10.3390/electronics8121435.

[40] “Link Labs,” SigFox Vs. LoRa: A Comparison Between Technologies & Business Models, May 2018. https://www.link-labs.com/blog/sigfox-vs-lora (accessed Sep. 15, 2020). [41] Sigfox, “Sigfox Technical Overview,” vol. 1, no. May, p. 26, 2017, [Online].Available:https://www.disk91.com/wpcontent/uploads/2017/05/4967675830228422064.pdf.

[42] R. Fujdiak et al., Security in low-power wide-area networks: state-of-the-art and development toward the 5G. INC, 2020.

[43] O. León, J. Hernández-Serrano, and M. Soriano, “Securing cognitive radio networks,” Int. J. Commun. Syst., vol. 23, no. 5, pp. 633–652, 2010, doi: 10.1002/dac.

[44] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, “Overview of Cellular LPWAN Technologies for IoT Deployment :,” pp. 197–202, 2018.

[45] R. S. Sinha, Y. Wei, and S. H. Hwang, “A survey on LPWA technology: LoRa and NB-IoT,” ICT Express, vol. 3, no. 1, pp. 14–21, 2017, doi: 10.1016/j.icte.2017.03.004.

[46] “Fraunhofer Institute for Integrated Circuits IIS.” https://www.iis.fraunhofer.de/en/ff/lv/net/telemetrie.html (accessed Sep. 15, 2019).

[47] K. Nolan and M. Kelly, “IPv6 convergence for IoT cyber-physical systems,” Inf., vol. 9, no. 4, 2018, doi: 10.3390/info9040070.

[48] A. O. Otuoze, M. W. Mustafa, O. O. Mohammed, M. S. Saeed, N. T. Surajudeen-Bakinde, and S. Salisu, “Electricity theft detection by sources of threats for smart city planning,” IET Smart Cities, vol. 1, no. 2, pp. 52–60, 2019, doi: 10.1049/iet-smc.2019.0045.

[49] “Kudelski Security Research,” Nov. 2017. https://research.kudelskisecurity.com/2017/11/21/zigbee-security-basics-part-3/ (accessed Apr. 15, 2019).

[50] “Pen test partners,” Z-Shave. Exploiting Z-Wave downgrade attacks, May 2018. https://www.pentestpartners.com/security-blog/z-shave-exploiting-z-wave-downgrade-attacks/ (accessed May 2020).

[51] C. Hennebert and J. Dos Santos, “Security protocols and privacy issues into 6LoWPAN stack: A synthesis,” IEEE Internet Things J., vol. 1, no. 5, pp. 384–398, 2014, doi: 10.1109/JIOT.2014.2359538.

[52] F. L. Coman, K. M. Malarski, M. N. Petersen, and S. Ruepp, “Security issues in internet of things: Vulnerability analysis of LoRaWAN, sigfox and NB-IoT,” Glob. IoT Summit, GIoTS 2019 - Proc., 2019, doi: 10.1109/GIOTS.2019.8766430.

[53] “Radware blog,” Protecting against Narrowband IoT Security Risks, Aug. 2019. https://blog.radware.com/serviceprovider/2019/08/protecting-against-narrowband-iot-security-risks/. (accessed Apr. 2020).

[54] R. Mattioli and K. Moulinos, “Communication network interdependencies in smart grids,” EUA FNAI Security, Ed., ed. EU: ENISA, 2015.

[55] “Cyber punk review,” The CIA’s latest claim: Hackers Have Attacked Foreign Utilities., Jan. 2008. http://www.cyberpunkreview.com/news-as-cyberpunk/the-cias-latest-claim-hackers-have-attacked-foreign-utilities/ (accessed Apr. 2019).

Chapter 2 References:

[1] S. Sezgin, “The Third Industrial Revolution: How Lateral Power is Transforming Energy, the Economy, and the World,” *Turkish Journal of Business Ethics*, 2018.

[2] Cao, J. /Yang, M. (2013): Energy Internet – Towards Smart Grid 2.0. Networking and Distributing Computing (ICNDC), Fourth International Conference IEEI.

[3] Tsoukalas, L. H./Gao, R. (2008): From smart grids to an energy internet: Assumptions, architectures and requirements. In: Proc. 3rd International Conference on Electric Utility Deregulation and Restructuring and Power Technologies.

[4] Vermesan, O. et al. (2011): Internet of Energy – Connecting Energy Anywhere Anytime. In: G. Meyer, J. Valldorf (Eds.): Advanced Microsystems for Automotive Applications 2011 DOI 10.1007/978-3-642-21381-6_4, © Springer-Verlag Berlin Heidelberg 2011.

[5] Zhou, K. /Yang, S. /Shao, Z. (2016): Energy internet: the business perspective. Applied Energy, 178, 212-222. Https: //bit.ly/2JhfHPm. Retrieved: 30.03.2018.

[6] W. J. Miller, "Internet of things (IOT) for Smart Energy Systems," *Smart Energy Grid Engineering*, pp. 237–244, 2017.

[7] Kafle, Y. R. /Mahmud, K. /Morsalin, S. /Town, G. E. (2016): Towards an Internet of Energy. IEEE conference, 2016.

[8] Rana, M. (2017): Architecture of the Internet of Energy Network: An Application to Smart Grid Communications. Volume 5, 17. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7891908 Retrieved: 18.04.2018 Internet of Energy: state of the art and scenarios at European level 17

[9] Zhou, J. /Ni, W. /Zhu, Z. (2017): Architecture of Energy Internet and Its Technologies in Application Reviewed. Journal of Clean Energy Technologies, Vol. 5, No. 4, July 2017 http://www.jocet.org/vol5/391-R0007.pdf Retrieved 20.04.2018

[10] Smart Grid Reference Architecture. CEN-CENELEC-ETSI Smart Grid Coordination Group, 2012.

[11] Huang, A. Q./Crow, M. L./Heydt, G. T. et al. (2011): The future renewable electric energy delivery and management (FREEDM) system: The energy internet, Proceedings of the IEEE, vol. 99, no. 1, pp. 133-148.

[12] NIST Framework and Roadmap for Smart Grid Interoperability Standards (2014): National Institute of Standards and Technology, US Department of Commerce 1108R3.

[13] Gellings, C. W. (1985): The concept of demand-side management for electric utilities. Proceedings of the IEEE, vol. 73, no. 10, pp. 1468-1470.

[14] Virtual Power Plant: Next Kraftwerke. https://www.next-kraftwerke.com/vpp/virtual-power-plant Retrieved 20.04.2018

[15] V. A. da Silva Gonçalves and F. J. M.-H. dos Santos, "Energy management system ISO 50001: 2011 and energy management for sustainable development," Energy Policy, vol. 133, p. 110868, 2019..

[16] P. Mancarella, "MES (multi-energy systems): An overview of concepts and evaluation models," Energy, vol. 65, pp. 1–17, 2014.

[17] Jyung, T. /Jeong K. /Baek, Y. et al. (2012): The system design and demonstration for autonomous microgrid operation. Journal of Electrical Engineering and Technology, vol. 7, no. 2, pp. 171-177.

[18] S. E. D. Coalition, “Mapping demand response in Europe today,” Tracking Compliance with Article, vol. 15, 2014.

[19] Short, J. A./Infield, D. G./Freris, L. L. (2007): Stabilization of grid frequency through dynamic demand control. IEEE Transactions on Power Systems, vol. 22, no. 3,

[20] Sternberg, A. /Bardow, A. (2015): Power-to-What? Environmental assessment of energy storage systems. Energy Environ. Sci., vol. 8, no. 2, pp. 389-400.

[21] van Gerwen, R. /Jaarsma, S. /Wilhite, R. (2006): Smart metering. KEMA Labortories.

[22] Q. Huang, S. Jing, J. Yi, and W. Zhen, Innovative testing and measurement solutions for smart grid. John Wiley & Sons, 2015.

[23] Y. Zhou, W. Ni, and Z. Zhu, “Architecture of energy internet and its technologies in application reviewed,” Journal of Clean Energy Technologies, vol. 5, no. 4, pp. 320–327, 2017.

[24] W. Haslbeck, M. Sojer, T. Smolka, and O. Brückl, “Mehr Netzanschlusskapazität durch regelbare Ortsnetztransformatoren,” etz, vol. 9, no. 2–7, p. 27, 2012.

[25] “BBC,”https://www.bbc.com/news/business-37220703, Aug.2016. https://www.bbc.com/news/business-37220703 (accessed Mar. 2020).

[26] C. Catalin-Felix, A. Mircea, V. Julija, M. A. Maria, F. Gianluca, and A. Eleftherios, “Smart grid projects outlook 2014,” 2014.

[27] Smart meters 101: France’s Linky electricity meters (2018): https://www.smart-energy.com/features-analysis/smart-meters-101-frances-linky-electricity-meters/ Retrieved 07.01.2019.

[28] A. Q. Huang, M. L. Crow, G. T. Heydt, J. P. Zheng, and S. J. Dale, “The future renewable electric energy delivery and management (FREEDM) system: the energy internet,” Proceedings of the IEEE, vol. 99, no. 1, pp. 133–148, 2010.

[29] W. Wang, Y. Xu, and M. Khanna, “A survey on the communication architectures in smart grid,” Computer networks, vol. 55, no. 15, pp. 3604–3629, 2011.

[30] Introduction to NISTIR 7628 guidelines for smart grid cyber security (2010): Grid, NIST Smart. Guideline.

[31] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. Wang, “Impact of cyber-security issues on smart grid,” in 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, 2011, pp. 1–7.

[32] S. Fries, H. J. Hof, T. Dufaure, and M. G. Seewald, “Security for the smart grid–enhancing IEC 62351 to improve security in energy automation control,” Int. J. Adv. Secur, vol. 3, no. 4, 2010.

[33] S. Karnouskos and O. Terzidis, “Towards an information infrastructure for the future internet of energy,” in Communication in Distributed Systems-15. ITG/GI Symposium, 2007, pp. 1–6

[34] "Germany Trade & Invest," Germany's Energy Concept. https://www.gtai.de/en/invest/industries/healthcare/germany-s-energy-concept-105260#105270 (accessed Apr. 2021).

[35] "Gesetz über den Messstellenbetrieb und die Datenkommunikation in Intelligenten Energienetzen;Messstellenbetriebsgesetz," MsbG. 2016. https://www.gesetze-im-internet.de/messbg/MsbG.pdf (accessed Feb. 2019).

[36] "Bundesamt für Sicherheit in der Informationstechnik. Technische Richtlinie BSI TR-03109-1: Anforderungenan die Interoperabilität der Kommunikationseinheit eines Intelligenten Messsystems" 2019. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR03109-1.pdf (accessed Feb 019).

[37] "Bundesamt für Sicherheit in der Informationstechnik. Certificate Policy der Smart Metering PKI"; 2017 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/PKI_Certificate_Policy.pdf (accessed 1 Feb 2019).

[38] "The European Parliament and European Council. Directive 2009/72/EC of the European Parliament and of the Council: Common Rules for the Internal Market in Electricity and Repealing Directive 2003/54/EC"; 2009 https://eur-lex.europa.eu/legal-content/en/ALL/?uri=celex%3A32009L0072 (accessed 1 Feb 2019).

[39] Bundestag. Gesetz zur Digitalisierung der Energiewende; Bundesanzeiger Verlag GmbH: Köln, Germany, 2016.

[40] D. Bundestag, Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz-MsbG). Bundesanzeiger Verlag GmbH Köln, Germany, 2016.

[41] N. Kroener, K. Förderer, M. Lösch, and H. Schmeck, "State-of-the-art integration of decentralized energy management systems into the German smart meter gateway infrastructure," Applied Sciences, vol. 10, no. 11, p. 3665, 2020.

[42] Bundesamt für Sicherheit in der Informationstechnik. Technische Richtlinie BSI TR-03109-1: Anforderungenan die Interoperabilität der Kommunikationseinheit Eines Intelligenten Messsystems; Bundesamt für Sicherheit in der Informationstechnik: Bonn, Germany, 2013.

[43] https://www.commoncriteriaportal.org/files/ppfiles/pp0073b_pdf.pdf

[44] Bundesamt für Sicherheit in der Informationstechnik. Technische Richtlinie BSI TR-03109-1: Anforderungen an die Interoperabilität der Kommunikationseinheit Eines Intelligenten Messsystems; Bundesamt für Sicherheit in der Informationstechnik: Bonn, Germany, 2013.

[45] N. Kroener, K. Förderer, M. Lösch, and H. Schmeck, "State-of-the-art integration of decentralized energy management systems into the German smart meter gateway infrastructure," Applied Sciences, vol. 10, no. 11, p. 3665, 2020.

[46] Bundesamt für Sicherheit in der Informationstechnik. Certificate Policy der Smart Metering PKI; Bundesamtfür Sicherheit in der Informationstechnik: Bonn, Germany, 2017.

[47] “European Commission, Joint Research Centre, Smart Electricity Systems and Interoperability. Smart Metering Deployment in the European Union”, https://ses.jrc.ec.europa.eu/smartmetering-deployment-european-union (accessed 19 Mar 2019).

[48] U. Greveler, “Die smart-metering-debatte 2010–2016 und ihre ergebnisse zum schutz der Privatsphäre,” Datenbank-Spektrum, vol. 16, no. 2, pp. 137–145, 2016.

[49] M. Hoefling, F. Heimgaertner, D. Fuchs, and M. Menth, “jOSEF: A Java-Based Open-Source Smart Meter Gateway Experimentation Framework,” in DA-CH Conference on Energy Informatics, 2015, pp. 165–176.

Chapter 3 References:

[1] “P. Gordon, “Russia attacked the US power grid. what if they don't stop?,” Smart Energy International, 23-Jul-2018, https://www.smart-energy.com/regional-news/north-america/russia-attacked-the-us-power-grid-what-if-they-dont-stop/ (accessed: Sep 2022]

[2] L. Specification, “The authors reserve the right to change specifications without notice. LoRa Specification 2 NOTICE OF USE AND DISCLOSURE 5,” 2015.

[3] Vitiello, S, Vasiljevksa, J, Filiou, C, “Cost-benefit analyses & state of play of smart metering deployment in the EU-27,” 2014.

[4] S. Ghosh, M. Pipattanasomporn, and S. Rahman, “Technology deployment status of U.S. smart Grid projects - Electric distribution systems,” 2013 IEEE PES Innov. Smart Grid Technol. Conf. ISGT 2013, 2013, doi: 10.1109/ISGT.2013.6497867.

[5] J. Twentyman, “Chateau Kefraya cultivates smart vineyard pilot in Lebanon,” *Internet of Business*, 29-Nov-2017, https://internetofbusiness.com/chateau-kefraya-cultivates-smart-vineyard-lebanon (accessed: Sep 2020]

[6] U. Nations and S. Division, “Technical assistance to Lebanon on improving energy statistics for sustainable development : Assessment mission report,” no. July, 2019.

[7] Link Labs, “Low Power, Wide Area Networks networks (LPWANs),” vol. 19, no. 2, pp. 855–873, 2017.

[8] 18th A. 2018, “IOT connectivity options: Comparing short-, long-range technologies,” IoT World Today, https://www.iotworldtoday.com/2018/08/19/iot-connectivity-options-comparing-short-long-range-technologies/ (accessed: Mar 2020)

[9] R. S. Sinha, Y. Wei, and S. H. Hwang, “A survey on LPWA technology: LoRa and NB-IoT,” ICT Express, vol. 3, no. 1, pp. 14–21, 2017, doi: 10.1016/j.icte.2017.03.004.

[10] M. Bloechl, “SigFox vs. Lora: Technologies & Business Models: Link Labs,” *SigFox vs. LoRa: Technologies & Business Models | Link Labs*, http://www.link-labs.com/blog/sigfox-vs-lora (accessed: Mar 2021)

[11] “Lora vs LTE: Lora advantages over cellular and Local Area Networks,” *3GLTEInfo*, 20-Jul-2016, http://www.3glteinfo.com/lora/lora-advantages/ (accessed: Sep-2020)

[12] M. Bloechl, “SigFox vs. Lora: Technologies & Business Models: Link Labs,” *SigFox vs. LoRa: Technologies & Business Models | Link Labs*, http://www.link-labs.com/blog/sigfox-vs-lora (accessed: Jul 2021]

[13] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, “Overview of Cellular LPWAN Technologies for IoT Deployment ,” pp. 197–202, 2018.

[14] L. Germani, V. Mecarelli, G. Baruffa, L. Rugini, and F. Frescura, “An IoT architecture for continuous livestock monitoring using lora LPWAN,” Electron., vol. 8, no. 12, 2019, doi: 10.3390/electronics8121435.

[15] “Lora¶,” LoRa, https://lora.readthedocs.io/en/latest/ (accessed: Apr 2020).

[16] “Lora Shield,” Lora Shield - Wiki for Dragino Project, https://wiki1.dragino.com/index.php?title=Lora_Shield. (accessed:1 Sep 2021)

[17] “Raspberry Pi Lorawan Gateway,” Instructables, 19-Dec-2018, https://www.instructables.com/Raspberry-Pi-LoRaWAN-Gateway. (accessed: 15 Sep 2021)

[18] N. Blenn and F. Kuipers, “Lorawan in the wild: Measurements from the things network,” arXiv.org, 09-Jun-2017, https://arxiv.org/abs/1706.03086 (accessed: 1 Sep 2021)

[19] “What is lorawan® specification,” LoRa Alliance®, 25-Jun-2022. [Online]. Available: https://lora-alliance.org/about-lorawan/ (accessed: 15 Apr 2022) .

[20] X. Yang, “LoRaWAN: Vulnerability analysis and practical exploitation,” Delft University of Technology. Master of Science, 2017.

[21] L. Pierce, *LoRa Mote User’s Guide*. 2016.

[22] R. Sanchez-Iborra, J. Sánchez-Gómez, S. Pérez, P.J. Fernández, J. Santa, J.L. Hernández-Ramos, A.F. Skarmeta, “Enhancing lorawan security through a lightweight and authenticated key management approach,” Sensors, vol. 18, no. 6, p. 1833, 2018.

Chapter 4 References:

[1] P. Gordon, “Russia attacked the US power grid. what if they don't stop?,” Smart Energy International, 23-Jul-2018 https://www.smart-energy.com/regional-news/north america/russia-attacked-the-us-power-grid-what-if-they-dont-stop (accessed: Sep 2022)

[2] N. Nhede, “Just 153.3 million Lpwan Smart Meters from 2019 – 2028,” Smart Energy International, 16-Jan-2020 https://www.smart-energy.com/industry-sectors/smart-meters/just-153-3-million-lpwan-smart-meters-from-2019-2028 (accessed: Sept 2021)

[3] G. Barnicoat and M. Danson, “The aging population and smart metering: A field study of householders’ attitudes and behaviours towards energy use in Scotland,” Energy Res. Soc. Sci., vol. 9, pp. 107–115, 2015, doi: 10.1016/j.erss.2015.08.020.

[4] W. Wang, Y. Xu, and M. Khanna, “A survey on the communication architectures in smart grid,” Comput. Networks, vol. 55, no. 15, pp. 3604–3629, 2011, doi: 10.1016/j.comnet.2011.07.010.

[5] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, W.H. Chin, “Smart grid communications: Overview of research challenges, solutions, and standardization activities,” IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 21–38, 2012.

[6] “Open smart grid protocol,” Wikipedia, 14-Dec-2018. http://en.wikipedia.org/wiki/Open_smart_grid_protocol (accessed: Aug 2021)

[7] C. Specification, “for Energy Metering DLMS / COSEM Architecture and Protocols,” pp. 1–310, 2009, [Online].

[8] “Device language message specification,” DLMS, https://www.dlms.com/home (accessed: Feb-2021)

[9] C. Specification, “for Energy Metering Blue Book Edition 12 . 2 and OBIS Object Identification System DLMS User Association,” pp. 1–229, 2017.

[10] V. C. Güngör et al., “Smart grid technologies: Communication technologies and standards,” IEEE Trans. Ind. Informatics, vol. 7, no. 4, pp. 529–539, 2011, doi: 10.1109/TII.2011.2166794.

[11] A. A. Khan, M. H. Rehmani, and M. Reisslein, “Cognitive Radio for Smart Grids : Survey of Architectures, Spectrum Sensing Mechanisms , and Networking Protocols,” no. c, pp. 1–41, 2015, doi: 10.1109/COMST.2015.2481722.

[12] H. Hu, D. Kaleshi, A. Doufexi, and L. Li, “Performance analysis of IEEE 802.11af standard based neighbourhood area network for smart grid applications,” IEEE Veh. Technol. Conf., vol. 2015, pp. 0–4, 2015, doi: 10.1109/VTCSpring.2015.7146000.

[13] L. Germani, V. Mecarelli, G. Baruffa, L. Rugini, and F. Frescura, “An IoT architecture for continuous livestock monitoring using lora LPWAN,” Electron., vol. 8, no. 12, 2019, doi: 10.3390/electronics8121435.

[14] R. S. Sinha, Y. Wei, and S. H. Hwang, “A survey on LPWA technology: LoRa and NB-IoT,” ICT Express, vol. 3, no. 1, pp. 14–21, 2017, doi: 10.1016/j.icte.2017.03.004.

[15] “LoRa Documentation,” 2019.

[16] M. Foti and M. Vavalis, “Jo l P re of,” Blockchain Res. Appl., p. 100008, 2021, doi: 10.1016/j.bcra.2021.100008.

[17] K. Agavanakis, P. G. Papageorgas, G. A. Vokas, D. Ampatis, and C. Salame, “Energy trading market evolution to the energy internet a feasibility review on the enabling internet of things (IoT) cloud technologies,” AIP Conf. Proc., vol. 1968, 2018, doi: 10.1063/1.5039264.

[18] P. G. Papageorgas, K. Agavanakis, I. Dogas, and D. D. Piromalis, “IoT gateways, cloud and the last mile for energy efficiency and sustainability in the era of CPS expansion: "a bot is irrigating my farm.. ",” AIP Conf. Proc., vol. 1968, 2018, doi: 10.1063/1.5039262.

[19] Q. Wang, R. Li, and L. Zhan, “Blockchain technology in the energy sector : From basic research to real world applications,” Comput. Sci. Rev., vol. 39, p. 100362, 2021, doi: 10.1016/j.cosrev.2021.100362.

[20] N. Chinchilla-Romero, J. Navarro-Ortiz, P. Muñoz, and P. Ameigeiras, “Collision avoidance resource allocation for LoRaWAN,” Sensors (Switzerland), vol. 21, no. 4, pp. 1–19, 2021, doi: 10.3390/s21041218.

[21] “Gurux for DLMS Smart Meters,” Gurux.DLMS | Gurux for DLMS smart meters. http://www.gurux.fi/Gurux.DLMS (accessed: Jun 2021)

Chapter 5 References

[1] “Raspberry Pi,” Wikipedia. Mar. 09, 2021. Accessed: Mar. 09, 2021, https://en.wikipedia.org/w/index.php?title=Raspberry_Pi&oldid=1011126050

[2] “ESP32 MCU.” https://www.espressif.com/en/products/socs/esp32 (accessed Mar. 2021).

[3] A. Ltd, “ARM Home Page,” Arm |The Architecture for the Digital World. https://www.arm.com/ (accessed Mar. 09, 2021).

[4] “RISC-V Home Page,” RISC-V International. https://riscv.org/ (accessed Mar 2021).

[5] V. Deshpande, H. Badis, and L. George, “BTCmap: Mapping bitcoin peer-to-peer network topology,” 2018 IFIP/IEEE Int. Conf. Perform. Eval. Model. Wired Wirel. Networks, PEMWN 2018, no. August 2016, pp. 6–11, 2018, doi: 10.23919/PEMWN.2018.8548904.

[6] S. Haber and S. Stornetta, “How to timestamp a digital document - original blockchain paper 1991,” J. Cryptol., vol. 3, no. 2, pp. 99–111, 1991.

[7] I. O. Adam and M. Dzang Alhassan, “Bridging the global digital divide through digital inclusion: the role of ICT access and ICT use,” Transform. Gov. People, Process Policy, vol. 15, no. 4, pp. 580–596, 2020, doi: 10.1108/TG-06-2020-0114.

[8] V. Deshpande, L. George, and H. Badis, “SaFe: A Blockchain and Secure Element Based Framework for Safeguarding Smart Vehicles,” Proc. 12th IFIP Wirel. Mob. Netw. Conf. WMNC 2019, pp. 181–188, 2019, doi: 10.23919/WMNC.2019.8881408.

[9] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” p. 9.

[10] “Remix - Ethereum IDE & community,” Remix - Ethereum IDE & community. https://ethereum.github.io/ (accessed May 2021).

[11] “Ganache,” Truffle Suite. https://trufflesuite.com/ganache (accessed May 2021).

[12] Global Platform, “Introduction to Secure Elements,” no. May, p. 9, 2018, www.globalplatform.org.

[13] P. Urien, “RACS: Remote APDU call secure creating trust for the internet,” 2015 Int. Conf. Collab. Technol. Syst. CTS 2015, pp. 351–357, 2015, doi: 10.1109/CTS.2015.7210448.

[14] V. Deshpande, L. George, and H. Badis, “Pulsec: Secure Element based framework for sensors anomaly detection in Industry 4.0,” IFAC-PapersOnLine, vol. 52, no. 13, pp. 1204–1209, 2019, doi: 10.1016/j.ifacol.2019.11.362.

[15] V. Deshpande, T. Das, H. Badis, and L. George, “SEBS: A Secure Element and Blockchain Stratagem for Securing IoT,” 2019 Glob. Inf. Infrastruct. Netw. Symp. GIIS 2019, 2019, doi: 10.1109/GIIS48668.2019.9044957.

[16] “Multos Smartcard Technology,” Multos, 12-Jul-2021.

https://multos.com/technology/multos-smartcard-technology/ (accessed: June 2021)

[17] M. Foti and M. Vavalis, “What blockchain can do for power grids?” Blockchain: Research and Applications, p. 100008, Feb. 2021, doi: 10.1016/j.bcra.2021.100008.

[18] Q. Wang, R. Li, and L. Zhan, “Blockchain technology in the energy sector: From basic research to real world applications,” Computer Science Review, vol. 39, p. 100362, Feb. 2021, doi: 10.1016/j.cosrev.2021.100362