Expertise
and insight
for the future

Terho Craven

Advanced IoT solution for EV CHAdeMO Fast Charging Applied with Mobile Networks

Metropolia University of Applied Sciences

Bachelor of Engineering

Degree Programme in Information and Communication Technology

Bachelor’s Thesis

6 May 2019

Author Title Number of Pages Date	Terho Craven Advanced IoT solution for EV CHAdeMO Fast Charging Applied with Mobile Networks 34 pages + 1 appendices 6 May 2019
Degree	Bachelor of Engineering
Degree Programme	Information and Communication Technology
Professional Major	Communication Networks and Applications
Instructors	Jukka Anttonen, CEO Jukka Louhelainen, Senior Lecturer

This thesis covers important topics about electric charging infrastructure, research and development work progress as well as related areas and compares different solutions. The objective of this project is to create a new compact fast charging station with Unified Chargers company. It needs to have features that are not available at the market and it is made smart with the Internet of Things. Currently there are not enough charging stations to meet the future on-road electric vehicles (EV). Although, electric cars are most of the time being charged at home overnight, still the need for charging cars on-the-go is going to be growing when driving longer distances.

This study is based on the CHAdeMO standard, ENISA's best practices, reverse engineering and documentations of frameworks and cloud services. The reason for selecting these study materials was to find a possible way to produce the charging station with different approaches and make them secure.

The findings of this study showed that it is possible to find a way to update data to user without needing the charging station display and the unsecure RFID tags. Also, the Cloud can be used to provide extra freedom to work with.

The outcome was successful as the charging station was able to charge the EV from the mobile app that was authenticated. The application was able to get real-time data from the EV and perform start and stop. Earlier the company didn't have any Cloud IoT solution, but now the product has a working base functionality. The product can be further improved, and more features built on top of the current setup.

Keywords	IoT, Cloud, Mobile networks, Charging station & EV

Tekijä Otsikko Sivumäärä Aika	Terho Craven Advanced IoT solution for EV CHAdeMO Fast Charging Applied with Mobile Networks 34 sivua + 1 liitettä 6.5.2019
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Tieto- ja viestintätekniikan tutkinto-ohjelma
Ammatillinen pääaine	Tietoverkot ja Sovellukset
Ohjaajat	Toimitusjohtaja Jukka Anttonen Lehtori Jukka Louhelainen

Tämä insinöörityö kattaa tärkeitä aiheita sähkölatauksen infrastruktuurista, tuote ja kehitystyön kulusta ja siihen kuuluvista aihealueista sekä vertailee eri ratkaisumalleja. Projektin tavoite on luoda uusi kompakti nopea latausasema Unified Chargers yrityksen kanssa, jonka ominaisuuksia ei ole markkinoilla ja tehdä niistä älykkäitä asioiden internetin kanssa. Tällä hetkellä ei ole tarpeeksi latausasemia vastaamaan tulevaisuuden tiekäyttöisiä sähköautoja. Kuitenkin, suurin osa sähköautoista ladataan kotona yön yli, mutta silti tarvittava määrä kasvaa pidempien ajomatkojen kertyessä.

Tutkimus perustuu CHAdeMO standardiin, ENISA:n parhaisiin käytäntöihin, takaisinmallinnukseen sekä viitekehyksien ja pilvipalveluiden dokumentaatioihin. Oppimateriaalin tarkoitus oli löytää erilaisia mahdollisia ratkaisuja luoda latausasema turvallisesti.

Tutkimuksen löydökset osoittivat, että on mahdollista löytää keino päivittää dataa käyttäjälle ilman latausaseman näyttöä tai haavoittuvaista RFID tägiä. Pilvipalveluita voi myös käyttää luomaan ylimääräistä vapautta työskennellessä.

Lopputulos oli hyvä, kun latausasema saatiin lataamaan sähköauto todennetulla mobiili applikaatiolla. Applikaatio sai reaaliaikaista dataa sähköautolta ja pystyi suorittamaan käynnistä ja pysäytä toiminnot. Yrityksellä ei vielä ollut pilvipalvelu pohjaista asioiden internet ratkaisua, mutta nyt on toimiva peruspohjainen ratkaisu. Tuotetta pystyy vielä jatkokehittämään sekä luomaan uusia toimintoja nykyisen ratkaisun päälle.

Avainsanat	IoT, Cloud, Mobiiliverkot, Latausasema & sähköauto

Contents

Appendices

List of Figures

List of Abbreviations

A Ampere(amp). Unit value of electric current in the International System of Units.

AC Alternative Current. Electric current, that repeatedly reverses direction.

API Application Programming Interface. A set of information values to define program functionality to communicate with opposite program and exchange the values according to mutual interaction between the two.

App Application for running a task or job in mobile phones or tablets.

BEV Battery Electric Vehicle. Fully functional vehicle using only electric to operate.

CAN Controller Area Network. Vehicle bus standard for devices and microcontrollers, which supports communication between each application without a controlling host device.

CCS Combined Charging System. Direct Current Fast Charge standard. Based on J1772 standard and PLC communication.

CHAdeMO CHArge de MOve. Direct Current Fast Charge standard. Uses CAN bus communication.

CP Control Pilot. Communication line to adjust the vehicle charging rate.

CSQ Carrier Squelch. Suppresses the receiver audio of the desired RF signal.

DB Database. Organized library of compilations of data, which are stored and accessed electronically in a server.

dBm Desibel-milliwatt. Unit to measure power ratio expressed in decibel with reference to a milliwatt. Used in different wireless technologies.

DC Direct Current. Electric charge, which flows unidirectionally.

DCFC Direct Current Fast Charge. Level 3 charging that connects directly to electric car’s battery.

DoS Denial-of-Service. Cyber-attack to cause systems, information, devices or networking services to become unavailable for its users.

ENISA European Union Agency for Network and Information Security. Contributor of high-level network and information security recommendations, policies, implementations and collaborates directly with teams in EU.

EV Electric Vehicle. Vehicle that operates with one or more electric motors.

EVSE Electric Vehicle Supply Equipment. Typically, a charging station or charging dock. Controlling unit between the electric car and power grid.

FCEV Fuel Cell Electric Vehicle. Rather than using batteries, fuel cell electric vehicle uses fuel cells to generate electricity with oxygen and compressed hydrogen to the motor.

HEV Hybrid Electric Vehicle. Combination of internal combustion vehicle and electric propulsion system.

HTTP Hypertext Transfer Protocol. Application protocol used for data communication for the World Wide Web.

HTTPS Hypertext Transfer Protocol Secure. Encrypted on top of Hypertext Transfer Protocol (HTTP) secure communication with Secure Sockets Layer (SSL) protocol or Transport Layer Security (TLS).

Hz Hertz. Unit value of frequency in the International System of Units.

IaaS Infrastructure as a Service. Servers and networking for the Cloud. Baseline level for other Cloud services.

ICE Internal Combustion Engine. In a heat engine, combustion of oxidizer and fuel supply as the working fluids of the engine.

IoT Internet of Things. Embedded computing devices that are connected to the Internet. Sending and receiving data between IoT device and the other end.

IP Internet Protocol. Internet layer protocol, which takes care of packet transfer through the Internet. Essential for working Internet.

J1772 Alternative Current (AC) power charging connection standard by SAE.

JSON JavaScript Object Notation. Data interchange format, which is designed for humans to easily read and write. Structures based on collections of names and values pairs and ordered list of values.

kW KiloWatt. Unit value of power equal to one thousand watts.

kWh KiloWatt/hour. Energy used consistently over an extent of time. Commonly used for billing energy of consumed energy by consumers.

LED Light Emitting Diode. Two-lead semiconductor light source for indicating that something happened or used as light source with low energy consumption.

Li-ion Lithium-ion Battery. Rechargeable batteries used in variety of electric products.

LTE Long Term Evolution. Wireless broadband communication standard for mobile devices. Increased capabilities from UMTS.

M2M Machine to Machine. Two machines transferring data between each other without human interfacing or interaction.

MITC Man In The Cloud. Hacking attack term for targeting Cloud services and applications.

N Neutral. Carries current back to the source. Usually connected to ground.

NAT Network Address Translation. Method to assign public addresses into a private network of the firewall. Main job of the NAT is to limit number of unwanted public addresses to join the network of the organizations, companies and so on.

OCPP Open Charge Point Protocol. Charging station network protocol for central management system and communication between electric vehicle charging stations.

PaaS Platform as a Service. Platforms run by the Cloud such as analytics, tools and operating systems.

PE Protective Earth. Charge current flows to earth when failure occurs.

PHEV Plug-In Hybrid Electric Vehicle. Vehicle’s battery can be charged by charging stations or other electric power sources and by electric car’s own on-board engine and generator.

PLC Power-Line Communication. Communication technology for transferring data over existing power cables.

PoV Point of View. As seeing from someone’s perspective.

PP Proximity Pilot. Counters any unwanted actions while electric car is connected to charging resource.

PPP Point-to-Point Protocol. Data link layer communication protocol to set up a direct connection between two nodes.

QoS Quality of Service. Measurement of the overall performance of a service.

R&D Research and Development. Innovation and improvement of products and procedures.

RC Rapid Charge/r. AC and DC chargers, that will charge 80% of battery in 30 minutes.

RESTful Representational State Transfer-ful. Representational State Transfer architecture-based design for web service interaction between the computer systems.

RFID Radio-Frequency Identification. Radio wave using objects, which operates electromagnetic fields to automatically track and identify attached tags.

RSSI Received Signal Strength Indicator. Measurement unit for received radio signal.

SaaS Software as a Service. Software run by the Cloud without the need of installing the software itself on own device.

SAE Society of Automotive Engineers International. Creates automotive standards, education, professional certifications and competitions.

SDK Software Development Kit. Software development toolset for creating applications to software packages, platforms and frameworks.

SoC State of Charge. Electric vehicle's state of battery remaining percentage until next needed recharge.

SSH Secure Shell. Cryptographic protocol for remote command line networking connection.

SSL Secure Sockets Layer. Cryptographic protocol for networking to secure communication.

TLS Transport Layer Security. Cryptographic protocol for networking to secure communication. Similar to Secure Sockets Layer (SSL) protocol, but more secure protocol.

UMTS Universal Mobile Telecommunications System. Network standard for mobile cellular systems. Based on standard of Global System for Mobile communications.

V2G	Vehicle-to-Grid. Communication between power grid and selling the electricity based on distribution network.
W	Watt. Unit value of power.
ZEV	Zero-Emission Vehicle. Vehicle that diffuses no exhaust gas pollution.
XML	Extension Markup Language. Encodes documents to a format in human and computer readable way. Used in Application Programming Interfaces.

1 Introduction

The purpose of this thesis project is to research the possibility to create an Internet of Things (IoT) solution for a fast charging station, which would be compact and smart for commercial and private usage. Most current fast charging stations are huge and work with only one Electric Vehicle (EV) at a time, meaning waste of money and space per parking slot. Creating a compact station, which is made in Finland that charges two EVs at the same time and without needing an external power unit station would be more efficient. Also, solving the problem of knowing when the EV is charged without being near the station was a goal to achieve. The stations have displays to show limited amount real-time data, but mobile apps are not updating values as lots of commercial mobile apps are missing the functionalities of updated data from EV.

The project was done for Unified Chargers, which is an R&D start-up company of many talents from innovators to law. The main aim of the company currently is to build one of the most compact fast charging station for EVs. Standards used for the fast charging station are Combined Charging System (CCS) and CHArge de MOve (CHAdeMO). The charging station has been developed in Finland in co-operation with Aalto University and other manufacturers.

The primary interests for the thesis project were:

- Research and Development (R&D)
- Keep security and best practices in design perspective
- Read car and controller data + Send the read data to IoT Core
- Build an IoT solution to work, and so making it reliable for customers to use in day-to-day option to charge their own EVs
- Create a Cloud service using IoT platform and communicate with mobile app via APIs
- Work on mobile networks to create a cableless network for charging station, thus making new possibilities in terms of location

After this Introduction, Chapter 2 provides brief background theory and an overview of EV and charging station needs as well as Application Programming Interface (API) basic functioning used to move data around. Chapter 3 briefly describes the equipment and tools used. Chapters 4 to 6 go more deeply into the technology used, also their designs and security. Chapter 7 goes through the charging process from the user side and slightly more deeply in the background. Equivalent information of the charging station ecosystem is covered in chapter 8. The basics of different EV's and functions are covered in chapter 9. Lastly, chapter 10 and 11 go through the thesis findings and conclusion.

2 Background theory

This is a very brief look at the background theory of electric vehicles and charging station needs. Technology and the green way of driving is becoming a greater trend in this world's automobile driving. Electric Vehicles (EV) are increasing substantially, but the amount of fast charging solutions on the global map is still far from enough. How can this be solved in such a way that the technology becomes commercially available for a wider portion of the population? This is forcing more competition between the car manufacturers. Yet, upfront costs of the new Battery Electric Vehicles (BEV) are still quite high, but the electricity "fuel" of the BEV is cheaper than normal gasoline fuel [1]. Considerable challenges of BEV's include the driving range with current battery technology, charging time and location of the charging stations. Currently (October 2018) available BEVs battery range extends between 91.7 to 539 km (57 to 335 miles) [2]. Driving in cold weather affects the EV lithium-ion batteries (Li-on) capability and driving range. According to the American Automobile Association research, EV range can be reduced by an average of 41 percent while driving and using heating, ventilation and air-conditioning at the same time in -24 Celsius temperature [3]. Due to range issues, more charging stations are going to be needed.

API allows to communicate between programs and outsource the data to be used in 3rd party development. It allows internal and external API calls to function between e.g. mobile app and hardware. The functions can be designed to be public, private or partner based. These allow different kind of integrations, which should be pre-planned before deploying. With the information of APIs, the charging station manufacturers and 3rd party service providers may co-operate in creating the product and services together.

3 Basics of the electric car functions

Internal Combustion Engine (ICE) vehicles have been ruling for years before the era of various commercial EVs have gotten the limelight. Part of the reason is the climate change and reducing the oil usage. Even the ICE vehicles have slowly turned some of the functionalities into electric in the past years. A few good advantages of EVs are the cheaper "fuel" in short range daily use, no exhaust fumes and no need to maintain engine oil.

3.1 How the electric cars work

One of the main differences between an ICE car and EV is the electric motor, which replaces the gasoline engine. The electric motor's power source is a controller, also the responsible for torque. Controller gets its power from a rechargeable Li-ion battery that supplies the car overall functionality. The battery is located in the center of the EV, creating better driving handling due to center of gravity.

EVs are really quiet thanks to the electric motor. Charging happens from AC or DC power source, that usually is home outlet or installed EVSE. AC charging requires the use of on-board charger to change electricity to DC, which is used by the EV. There are AC motors also, but DC is simpler, cheaper and more common. Thermal cooling system takes care of cooling down the parts and components [4][5].

3.1.1 Different types of EVs

There are couple of different types of EV's that have more or less noticeable functional electrical and combination of gasoline solutions.

- **Battery Electric Vehicle (BEV)**. The “pure” EV that runs completely with electricity. Doesn’t pollute gas fumes due to its all electric functionality. Has AC and DC charging options depending on EV manufacturer [6].

- **Plug-in Hybrid Electric Vehicle (PHEV)**. Has both ICE and Electric motor. Working functionality with both of the motors but has usually lesser electric range. Better in longer distance trips due to its range and no anxiety of batteries running out [7].

- **Fuel Cell Electric Vehicle (FCEV)**. Moves with fuel cell stack that uses hydrogen to produce electricity. Similarly, to electric batteries fuel cells are electrochemical devices. Cells cannot be recharged like PHEV and BEV batteries, but refueled with supply of hydrogen in the same way as gasoline [7].

3.2 Zero emission vehicles

The Zero Emission Vehicle (ZEV) program was created in California as a regulation to car manufacturers to sell electric cars and trucks. The main objective was to ensure research and development for commercial vehicles to reduce global warming and no tailpipe pollution. In order to motivate producing EVs, the system involves vehicle credit formula for sold BEVs by their effectiveness. But, the main goal for the whole ZEV is to have vehicles pollute as few grams of CO_2e as possible [8].

4 Equipment and Tools

Essential components and services are briefly explained in this section. Usage of these equipment and tools will be covered more deeply in the next chapters. As this project is mostly working around the IoT solution, still the project would not work without its supporting components. A large variety of tools, technologies and programming were learned during the project progression.

4.1 Cloud

Choosing the right Cloud service for the project was based on a reliable and secure cloud provider. Cloud is creating many new possibilities of operating with less hardware, which requires fewer hardware upgrades and spending extra money into them. Hardware will be outdated in a matter of time and then needs to be thrown away. Since servers, backends and databases can be put to the Cloud, they will provide more freedom with high availability and scalability. Cloud services allow to use computing resources when needed or reserved for longer period. The pay rates depend on these choices.

The following *Figure 1* shows the basic concept of the cloud service used communicating between the EV charging station and the mobile app.

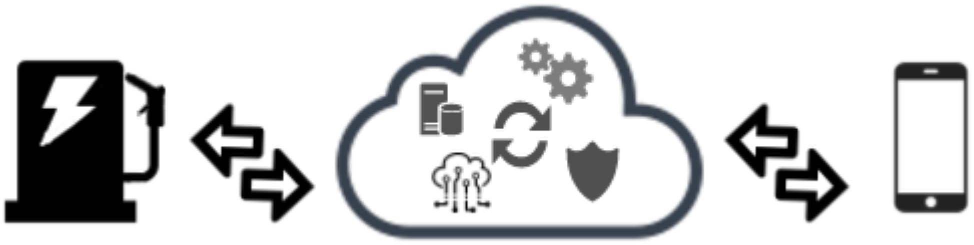


Figure 1 Cloud data exchange example

EV charging station runs its own backend code from the controller and communicates with Cloud via Message Queuing Telemetry Transport (MQTT) over Secure Sockets Layer (SSL), which works on top of the Transmission Control Protocol (TCP). This procedure adds extra layer of security for the applications and services to run over the internet for cybersecurity to prevent malicious attackers. This also applies to the connection between the cloud and mobile app. The app uses cloud provided Representational State Transfer-ful (RESTful) API's own Hypertext Transport Protocol (HTTP) requests to communicate commonly with either Extensible Markup Language (XML) or JavaScript Object Notation (JSON) content. The connection between them is secured via Hypertext Transport Protocol Secure (HTTPS) combined with Transport Layer Security (TLS) or Secure Sockets Layer (SSL) [9][10].

4.2 Charging station

A vital part of the project is the charging station. Without it, the project would not have been able to advance as the infrastructure was built around it. It can survive without cloud by adding external buttons for starting and stopping the charging with some design changes. However, in order to make it more advanced and competitive in the market in day-to-day use, the charging station needs a reliable Cloud and mobile app solution.

Figure 2 shows the Unified Chargers charging station (2018) and details.

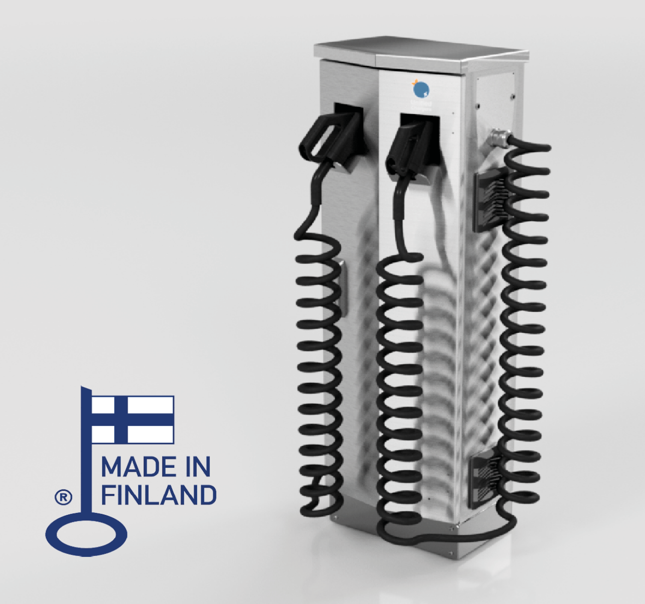


Figure 2 Unified Chargers charging station [11].

- Dimensions: 30 x 40 x 130 cm
- Weight: 80 kg
- Power: 22 kW
- Charging standards: CCS, CHAdeMO.

The charging station has curly cables, which allows the cables and the plugs to have less strain. Curly cables also solve the problem of current charging stations cables that are left hanging in messy way or just lying on ground. The station was also approved with Finnish key flag symbol. This means that more than 50% of the charging station production and designing has been done in Finland [12].

Figure 3 depicts Unified Chargers charging station's strongest points.

Innovation
Re-Branding
Reupdating data
Easy to install
Unified Chargers
Adjustable
Simple to use
Efficiency

Figure 3 Unified Chargers charging station strongest points

As seen in Figure 3, the charging station's strongest points have to do with easiness of installation, simplicity of use, efficiency and include features such as innovation, rebranding, and reupdating data. In addition, the station is adjustable.

4.3 Controllers

Controllers and microcontrollers are the heart of the physical hardware used in the charging station to prototype, test, build and recreate the hardware. The strong point with the controllers is the ability to run demanding tasks with low power and yet be compact sized.

Demands for the used controllers include:

- Able to connect to the Internet via Ethernet cable or mobile network
- Feed data without any delay throttles
- Controller Area Network (CAN) capability for CHAdeMO standard
- Power-Line Communication (PLC) capability for CCS standard
- Compact size and efficiency

With the required demands and right components found, the R&D work had a good start.

5 Cloud Infrastructure

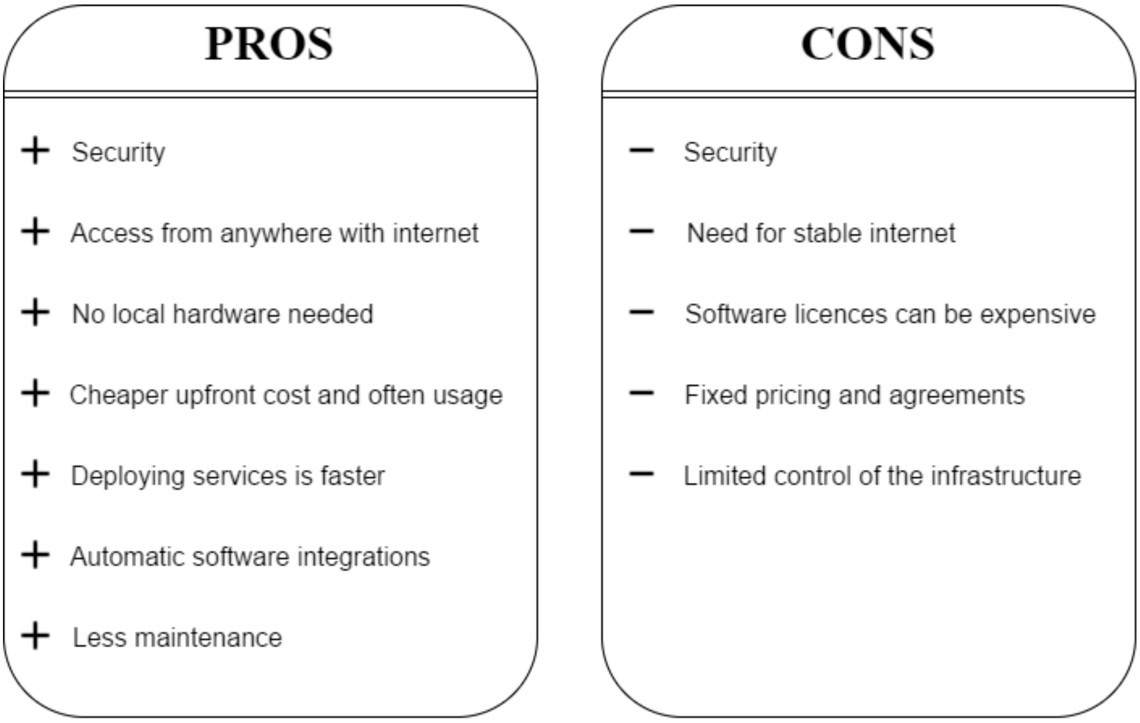
“Cloud computing is really a no-brainer for any start-up because it allows you to test your business plan very quickly for little money. Every start-up, or even a division within a company that has an idea for something new, should be figuring out how to use cloud computing in its plan.”

– Brad Jefferson, CEO and Co-Founder of Animoto.

According to the McAfee Navigating a Cloud Sky: Practical Guidance and the State of Cloud Security study from April 2018 by Raj Samani, 97 % of the organizations use cloud services. 65% have a cloud-first strategy, meaning that there is still some insecurity and uncertainty floating about the cloud when planning the first infrastructure. Also, the lack of cybersecurity specialists is slowing down the companies to adapt to the cloud and internet security in general.

When thinking of building a simple prototype or just to run computing service for a desired amount of time without any local hardware servers, then questions about using cloud services should arise. For example, trying out a new version, technology or running a backend for big or small project. Back in the old days, all of this required to have local hardware to store or compute something. Whenever this was running a database or moving data around multiple people. Whole process will cost less upfront as cloud service fees are priced by time, monthly or annual subscription by the usage of the services. Local hardware in other hand is usually one-time purchase with extra cost of support. On top of this, the local hardware will expire or get outdated in a matter of time. Thus, the hardware needs to be replaced into a new one and installed again [13].

The main advantages and disadvantages of cloud are listed in Figure 4.



PROS

+ Security

+ Access from anywhere with internet

+ No local hardware needed

+ Cheaper upfront cost and often usage

+ Deploying services is faster

+ Automatic software integrations

+ Less maintenance

CONS

− Security

− Need for stable internet

− Software licences can be expensive

− Fixed pricing and agreements

− Limited control of the infrastructure

Figure 4 Pros and cons of the cloud

As seen in Figure 4, Cloud security can be turned into a double-edged sword, and why is that? It is good to compare each Cloud service provider's offerings when choosing the right as there are a lot of different providers from open source to commercial giants. If the provider doesn't fulfill the compliances of the secure Cloud infrastructure, it may be that particular cloud is not suitable for the needs. Although, providers should maintain secure cloud infrastructure for the customers from datacenter hardware (OSI Layer 1 Physical) level to all the way to cloud application services (OSI Layer 7 Application), but this doesn't cover the human errors. Cloud provider contributes the tools to work with, but if the customer using it doesn’t configure the infrastructure correctly for own needs, then it might leave security holes to the infrastructure. For example, leaving ports open, information publicly open, weak passwords and not using extra layer of security such as multi-factor authentication are insecure practices [14][15][16].

One of the strongest use cases for the Cloud is its usage in wherever the internet is available. This makes mobile networking a powerful technology for Cloud-based applications to gain access to devices that are not located close to other Internet sources such as Wi-fi and ethernet. Yet, the internet connection needs to be stable enough to get the full benefits of using the Cloud services while on-going or being stationary.

Some companies also use hybrid Cloud, which operates partly as a private enterprise Cloud and a public Cloud. Enterprise Cloud allows applications to run and deploy much faster. For developers this gives more manageability and lower need for maintenance. Lastly, enterprise model has the fixed operating expenses [15].

5.1 Cloud

Cloud services can be categorized in three main services, which are the roots of the modern Cloud infrastructure. From the bottom to top, Infrastructure as a Service (IaaS) is the core for the services Platform as a Service (PaaS) and Software as a Service (SaaS). PaaS and SaaS are commonly used with IaaS in large scale projects, when using Cloud only infrastructure design. There are other services as well, but these three are the main focus. *Figure 5* shows the concept of services built on top of each layer [18].

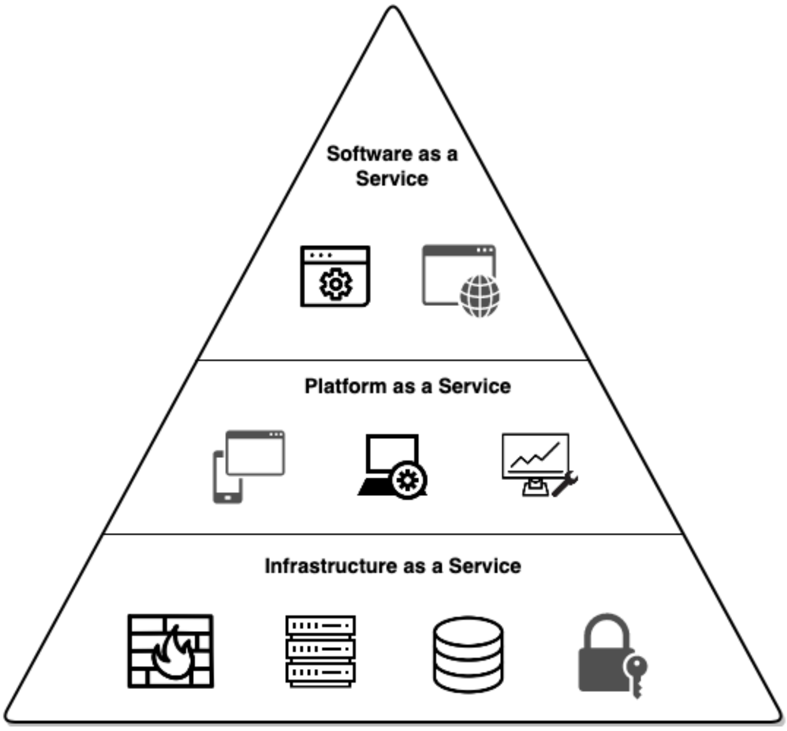


Figure 5 Cloud Infrastructure

The different layers of cloud infrastructure shown in Figure 5 are explained below.

IaaS consists of physical data centers, which hosts the Cloud services such as compute, storage and servers. These services run a data center monitoring, hardware, secure routing, certificates and firewalls such as Network Address Translation (NAT). IaaS has limited amount of privileges that the customer and provider can customize and configure. Servers, standard networking, firewalls and security are often maintained by the Cloud provider. Operating reliable security and maintenance of the Cloud ecosystem leaves less responsibilities for the customer to be complied with. A tremendous advantage of the IaaS is that the customer doesn’t need to first setup the whole infrastructure to start creating products [18][19][20].

PaaS takes advantage of ready-made solutions that requires manual installing and setup of tools or operating systems. For example, Cloud provider offers a virtual machine with set of compute power including processor cores, memory and storage. Run the virtual machine and it has all the compute set and a ready installed operating system. This can be done with a few mouse clicks instead of going through the old way of manual installing phases. Quick operating system setup allows to test multiple different systems, versions and computing power. Testing and developing products decreases time-to-market dramatically, increases the productivity and saves money from unnecessary physical hardware investments. For developers, PaaS is the backend platform for creating tools, analytics and core functions for the applications and software [18][21][22].

SaaS is the cherry on top of the cake, which allows developers quickly to deploy frontend content. For example, general SaaS products are email, websites and applications in cross-platform. By defining cross-platform, the user can use any operating system or web browser to access the content. Hosted SaaS products are available through the websites or program interfaces. Accessing the product content occurs without requiring installation of the application or program itself. Although, some may use plugins to connect between the device and application or software. Consumer doesn’t need to worry about controlling or managing the operating systems, servers, storage or network. Nowadays companies utilize the Cloud by creating software licensing for their products with time-based subscription. Subscription model is often based on monthly or yearly licensing. They are provided with updates and upgrades to keep the SaaS product alive and secure [18][23][24].

5.1.1 Design

Designing the Cloud infrastructure from vast available components and services that Cloud providers offer and update continuously can be tad difficult to begin with. New services pop-up weekly or even daily, which are somewhat similar or completely different from each other that run a specific task. Keeping up-to-date with trends such as IoT, machine learning and data analytics, the demand for multiple services in design is crucial [20]. Cloud providers often offer readymade services themselves or from third-party, which requires much less preconfiguration to begin developing and running services [18].

Common designing plan begins with an idea of which services are needed for a project. IaaS already provides the base configuration for simple base designs. More advanced projects tend get more complicated as the routing is done inside the manually configured private and public virtual Internet Protocol (IP) addresses. With the virtual IP addresses, Cloud designer can improve the infrastructure further by adding load balancers to reduce traffic flow into single service. When things go bad, implementing multiple zones to reroute the traffic from a faulty server, application or service will increases the uptime of the product and increases the stability of the infrastructure. Alternative zones replicate the exact data from main zone in real-time. When any of the zones go down, they will start recovering information from the other zone's replica copy in real-time. Upon completing the copying process, the zone will come up again and is available for its normal usage [18][26].

Below, Figure 6 shows most of the used services and their use cases.

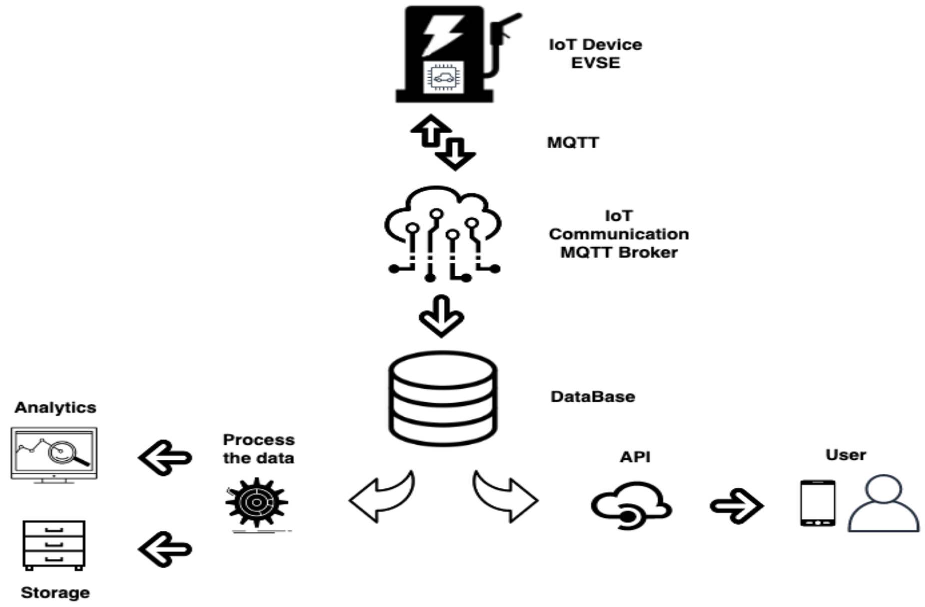


Figure 6 Cloud Design

As shown in Figure 6, the Cloud receives the data from Electric Vehicle Supply Equipment (EVSE) by subscribing to topics it provides. Data transfer itself between the IoT device and Cloud IoT Communication is based on the common lightweight messaging protocol Message Queuing Telemetry Transport (MQTT) standard, which communicates between publish and subscribe (More about MQTT in chapter 5). The subscribed message will be passed on to the MQTT broker, which will forward it to a designated database according to the settings made in the IoT Communication [27]. With the Cloud provider services, the data can be extracted to different data processes. Two main purposes for processing the data were analytics and storage. Analyzing the data helps to contribute more insight about the processes happening background, different charging behaviors, maintaining whole infrastructure and easing the problems troubleshooting. Purposes for storing the data are mostly for long-term documentation, analytical big data results and additional versioning. Database also transfers the content data to API. API surface gets the data in JSON format, which values will be used in developing the mobile app. Values are limited by the user privileges and the state in the charging process. For example, the user can be an owner of the EVSE and gain administration view. But, most of the visible data will be shown after the charging process has been validated with a token. Token authenticates the user during the charging process. The mobile app will then act as a portal to the user to operate the EVSE and charge their EV, get charging information and handle the billing.

5.1.2 Security

While the Cloud is expanding exponentially, also the threat of hacking attacks such as Man In The Cloud (MITC), Denial-of-Service (DoS) and Malware injection are increasing security risk matters. The big pile of data, which lies in the Cloud and gaining access to the systems is attracting hackers. Before, hacking would have needed more physical hardware fiddling and short-range data transfer, but the Internet makes the accessing easier without needing to worry about location [28][29]. A substantial amount of data breaches and leaks of private and business secrets, addresses, emails, passwords and behaviors have been mined by the hackers. Stolen data will be in most of the cases sold at deep web or so called “Internet’s black market” in chunks of millions of data sets for money or cryptocurrency.

How do you know if the Cloud Provider is secure enough? The answer is you don’t entirely know for sure, but you need to trust them by their reputation. As most of the Providers are public and not private, meaning they lack the private isolation of the infrastructure. Lots of the source code and documentation is available for hackers to find loopholes if the infrastructure is not configured securely enough. Public companies invest hefty amounts of money to hire the best engineers to keep the Cloud safe by preventing incoming malicious attacks and writing clean and secure code. Also, each external service working with the Cloud Provider signs the Service-Level Agreement (SLA) to ensure quality, security and responsibilities they hold as a 3rd party. Thus, partners, software and hardware are crucial part of the secure infrastructure for the end-users. Regulations and compliances such as the General Data Protection Regulation (GDPR) are monitoring the companies to apply best practices in their working culture to provide privacy driven future [30][31][32].

Securing own environment and the infrastructure for the end-users requires basic knowledge and training from the security specialists, and everyone that works in the same company. Simply having a weak password can lead to data leaks or in worst case scenario, to infrastructure infiltration and gaining access to valuable information or leaving backdoor for hacker to attack again. Best practice in most of the cases is common sense and doubting mindset to see multiple approaches. These are some of the best practices to keep end-user Point of View (PoV) secure.

- **Strong password**. Having a password, which is not found in dictionaries or simple and predictable as "password123" or linked to personal information, which can be found by search machines. Most of the users use same password in different platform, making them vulnerable for multiple hijacks. Creating at least 8-character long password with upper- and lower-case letters, numbers and symbols takes hacker much longer to crack the password through different combinations. For example, if just mentioned combination is used, the hacker would need to try go through 6,095,689,385,410,816 possible combinations. Comparing the last password possible combinations to 8-character password, which uses only letters is 208,827,064,57. First example makes the password 291,901 times harder to crack than the one with only letters. [33].

- **Identity and Access Management (IAM)**. To restrict access to limited tasks, maintenance, monitoring or administrating is good practice to reduce risk control in case of hacker gets unwanted access to a user account. Users get validated by the service and get access to specific operations based on the IAM configuration. For example, a database engineer has only access and modify permission to the databases, thus cannot read any other service information or modify them as they are out of the access configuration. IAM does audit logs of the user's actions, modifications, login times and attempts. If a hacker is trying to brute force in by trying different passwords, it would show up in audit log as failed login attempts. On top of IAM, it is highly suggested to add extra layer of security to user's password with Multi-Factor Authentication (MFA) for users and especially administrator permission authenticated users [34].

- **Encryption**. Encrypt as much of data as possible. Privacy is to be taken seriously as it can lead to unwanted data leaks such as personal information, passwords and website traffic sniffing. Encryption also prevents or slows down hackers who have stolen data, but strong enough encryption needs to be decrypted. Good practices to prevent IP traffic to is to encrypt with HTTPS, TLS, Secure Shell (SSH) and use of Virtual Private Network (VPN). VPN uses end-to-end tunneling private-public keypair to encrypt and decrypt IP packet traffic. In remote usage it relies on Point-to-Point Protocol (PPP), which establishes connection between two nodes. With the VPN, the open network data is secured with encryption and allows remote access to devices or access to geological restricted sites [34][35].

- **Web services security**. Web has a vast amount of "real appealing" sites and requests to open a link or insert user credentials via fake websites, email phishing attempts and "clickbait" pop-ups that lead to threat sites. Websites without HTTPS are also risky, because the web server to browser traffic is not encrypted with an SSL certificate. Certificates should also be approved by a trusted authority. VPN is highly recommended while browsing websites along with antivirus and firewall set up. Common sense is most important to prevent fishy appealing offers from email messages or if a random Uniform Resource Identifier (URL) link is safe to click. It's very likely that you haven't won the jackpot out of nowhere. To defend hackers to get in hosted services servers behind the scenes, which are open to world by ports e.g. HTTP port 80. It is best practice to not leave any unnecessary ports open, that would allow the attacker to gain access through different port [34].

6 Internet of Things

Almost anything that can be embeddable connected to the Internet is able to participate with the IoT ecosystem. A massive amount of different type of IoT devices have been created from small sensors to a smart city entity. The goal of the IoT is to automate daily tasks and get information from the sensors to improve industry effectiveness. Gaining data from different sources improves the analytical approach in the big data era. For example, the rubbish bin in the park is full. The IoT sensor attached to the bin has been programmed to sense the capacity with certain parameters. When reaching the point of bin being full, the IoT sensor sends the message to cleaning company and they will take out the trash. More or less simple and advanced IoT devices will change the world in the future and today, which creates a lot of opportunities and improvements to the society. Analyst firm Gartner has estimated 26 billion IoT connected devices by the year 2020. Huge increase in IoT devices has led to lots of the cheap commercial IoT devices. Cheap devices suffer from security issues as they have been created with haste and small budget. Having a small memory restricts creating a complex multilayer security in commercial used devices, but industrial devices are usually more secure [36][37].

The way IoT works, is based on Machine to Machine (M2M) and MQTT protocols. Two M2M devices communicates between each other wirelessly or wired. This allows them to connect into multi-device network and exchange the collected data to the end-point within a single network. MQTT itself was invented as a connectivity protocol for M2M by Dr. Andy Stanford-Clark in 1999. MQTT uses the publish-subscribe architecture exchange control packets between the broker and client. The control packets are kept as tiny as possible to maintain its lightweight transportation. Each packet consists of three parts, a payload, variable header and fixed header. Payload holds the data, which is being transported over the MQTT. Quality of the transportation is determined by the value of Quality of Service (QoS) [27][38][39][40]. There are three used QoS options for transporting the message:

1. QoS 0. At most once. The fastest quality as it delivers the message at most once or not at all. Message can be lost if the connection is cut as the message is not stored anywhere.

2. QoS 1. At least once. Unlike QoS 0, the message is stored locally by the sender until it receives a confirmation from receiver side. This makes sure that the message is delivered at least once, but there is a chance that the same message can be received multiple times if there has been failure before an acknowledgment.

3. QoS 2. Exactly once. The slowest and safest quality, since it requires longer handshaking and acknowledgement sequence to confirm the message transit compared to QoS 1. Message is stored locally similarly to QoS 1 and waits receiver to get information of successful publish. The message will be also stored in case of need to send the message again [41].

6.1.1 Design

The EVSE needs to be able to support both CHAdeMO's CAN and CCS's PLC communications to cover the market's EV base. In Figure 7, IoT Design, the IoT Device is designed to interact with Customer's EV and Cloud's IoT Communication. Cloud providers supply a Software Development Kit (SDK) for creating IoT applications.

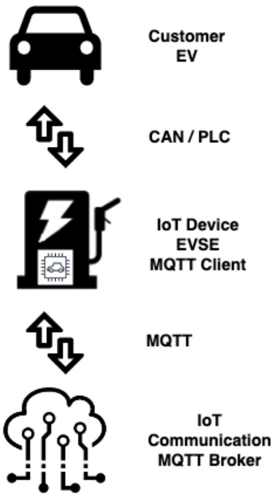


Figure 7 IoT Design

Customer with an EV will plug the car to EVSE and start the charging. The IoT Device will do the charging process according to the charging plug type. The Device will act as MQTT Client and is able to communicate with the Cloud's IoT Communication MQTT Broker with a X509 certificate.

6.1.2 Security

The European Union Agency for Network and Information Security (ENISA) and other security related companies have posted guidance and recommendation steps to secure IoT infrastructure and devices. Taking account how many IoT devices are available and in use at the moment is something, which can be a huge security risk in the wrong hands. Openly accessed devices are threat to both single user and to bigger audiences or industries. These devices can be linked together and communicate between each other. Hackers can take control of the devices and use them in large scale botnet Distributed DoS attacks. Attacks happen when legitimate users lose control of accessing devices, information systems or network resources. Targets commonly are services or hosts that rely on network access. Method for this is to flood the network server with requests until its traffic overloads the server and crashes. When hijacked IoT devices are being used as a part of botnet attack, the infection of the device is often unnoticed by its users. As there is not a complete solution to prevent the botnet DoS attack, a few precautious steps can still be taken to prevent the attack from happening [42][43][44]. These steps are such as:

- Use firewall to block incoming traffic. Configure unnecessary ports are closed and multiple requests are blocked.

- Have a trusted antivirus software.

- Disable unneeded communications such as Bluetooth.

- Sign up for DoS protection service to detect unusual traffic flow and redirect them away from the network.

- Secure important passwords and encrypt them.

- Multi-factor authentication, IAM and encrypted connections.

To keep the data safe between the IoT device and Cloud IoT Communication in MQTT publish-subscribe model is based on encrypted key-pair. TLS and SSL support a secure communication channel between a server and client by handshake mechanism to establish secure connection. The certificate for this matter is X509 certificate, which is provided by a trusted authority's server. Clients use the certificate to verify the identity of the server. A drawback from securing the connection comes in CPU usage and IP packet size increase, which requires bit more computing power [27][45]. Best practices for securing the MQTT connection between IoT Device and the Cloud are:

- Use TLS and the newest version of it whenever possible.
- Use trusted certificates instead of self-made.
- Avoid static typed passwords and credentials by all means.
- Block traffic to ports that are not necessary for MQTT.
- Keep software and libraries updates.
- Restrict root access and use SSH key-pair to remote access.

IoT is a trending technology, but manufacturers should take more proper action about the security risks to prevent malicious attacks. IoT devices can also be located in remote places. That is why they are often connected with mobile network to get the Internet connection. More about mobile network will be covered in the next chapter.

7 Mobile Network

The number of daily mobile users around the globe has increased the 3G Universal Mobile Telecommunications Service (UMTS) and 4G Long-Term-Evolution (LTE) demand and coverage map. 3G was introduced first time in 1998 and the 4G had its first appearance in 2008. The 3G network has been able to cover much more coverage compared to 4G making it more available in countries. According to the GSMA Intelligence, 3G coverage has increased from 75% to 87% globally between 2014 and 2017. The increase has added coverage for 1,1 billion people. Limiting factor of the coverage is the environmental difficulties in rural and remote areas, where installing and maintaining mobile network is hard to achieve. Meanwhile 4G coverage has doubled from 36% to 72% and covering additional 2,8 billion people [46]. Countries have diverse band frequencies from each other, meaning some of the cellular network using devices might not work in other country. It is good to acknowledge the frequency while purchasing devices from a vendor beforehand, so the full networking benefit gets in action. The United States and the rest of the world have slight differences in the 3G cellular band frequencies. United States uses 800/850/1700/1900/2100 MHz, meanwhile the rest of the world is using 850/900/1800/1900/2100 MHz frequencies [47].

PPP protocol allows to create simple links to transport packets between the 3G operator and IoT device. Simple links contribute full-duplex simultaneous bi-directional operations to deliver packets in order to establish the connection between the 3G operator and the IoT device. PPP uses link control protocol to validate that the link is valid for data transmission. The configuration is based on AT commands to match the connection information with the operator, such as access point name, SIM card PIN code and Carrier Squelch (CSQ) value. The AT+CSQ returns signal quality measurement, which is used in *Figure 8* to measure quality of the Received Signal Strength Indicator (RSSI). The decibel-milliwatts (dBm) is the unit to measure the RSSI [48][49][50][51].

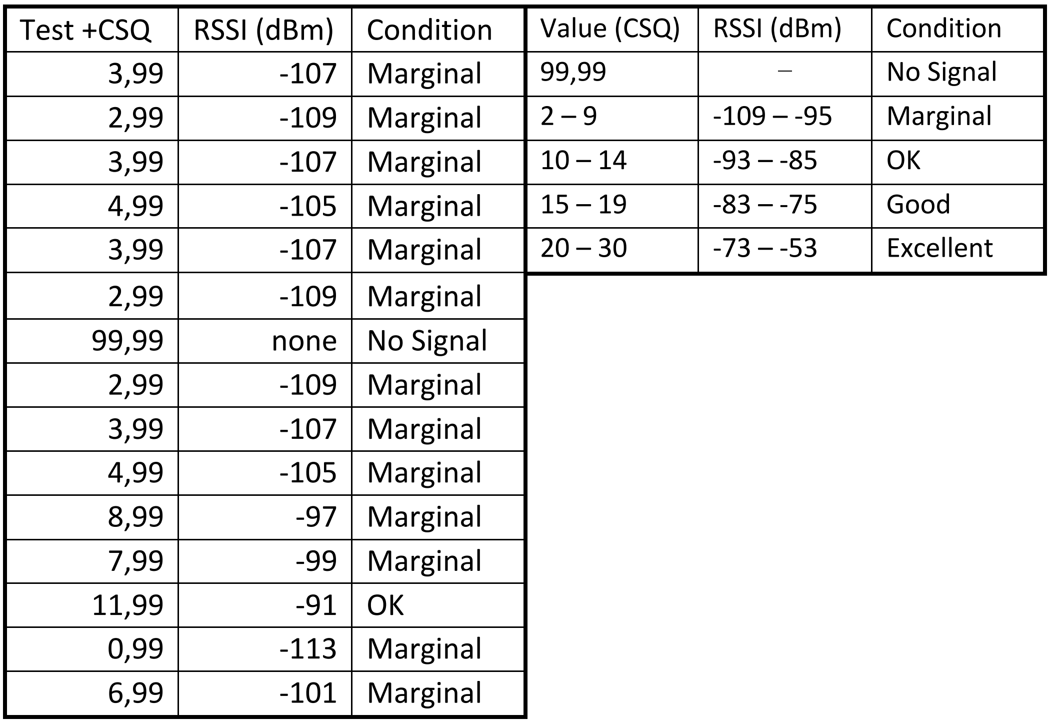
The following equation (1) shows the RSSI value. P_{mW} is the power of the access point signal:

$$P_{dBm} = 10\, x\, log_{10}{}^{(P_{mW})} \qquad (1)$$

P_{mW} heavily varies by the distance of the access point location [52].

Figure 8 shows the test results of measurements with old antennas to analyze the signal strength. The values are from build-in PPP AT+CSQ measurement tool, which is using the CSQ based equation (2):

$$RSSI\ (dBm) = (-113) + (2 * CSQ) \qquad (2)$$



Test +CSQ	RSSI (dBm)	Condition
3,99	-107	Marginal
2,99	-109	Marginal
3,99	-107	Marginal
4,99	-105	Marginal
3,99	-107	Marginal
2,99	-109	Marginal
99,99	none	No Signal
2,99	-109	Marginal
3,99	-107	Marginal
4,99	-105	Marginal
8,99	-97	Marginal
7,99	-99	Marginal
11,99	-91	OK
0,99	-113	Marginal
6,99	-101	Marginal

Value (CSQ)	RSSI (dBm)	Condition
99,99	–	No Signal
2 – 9	-109 – -95	Marginal
10 – 14	-93 – -85	OK
15 – 19	-83 – -75	Good
20 – 30	-73 – -53	Excellent

Figure 8 CSQ Test results on left and value conditions on right

CSQ does not have any measurement standard for its value, other than the manufacturer's announced value between 0 and 31 [53]. By changing the isotropic antenna, the RSSI can be amplified by the quality of the antenna or if possible, with multiple antennas to form multiple-input and multiple-output radio link method. Signal increase is announced in decibel-isotropic value by the antenna retailers.

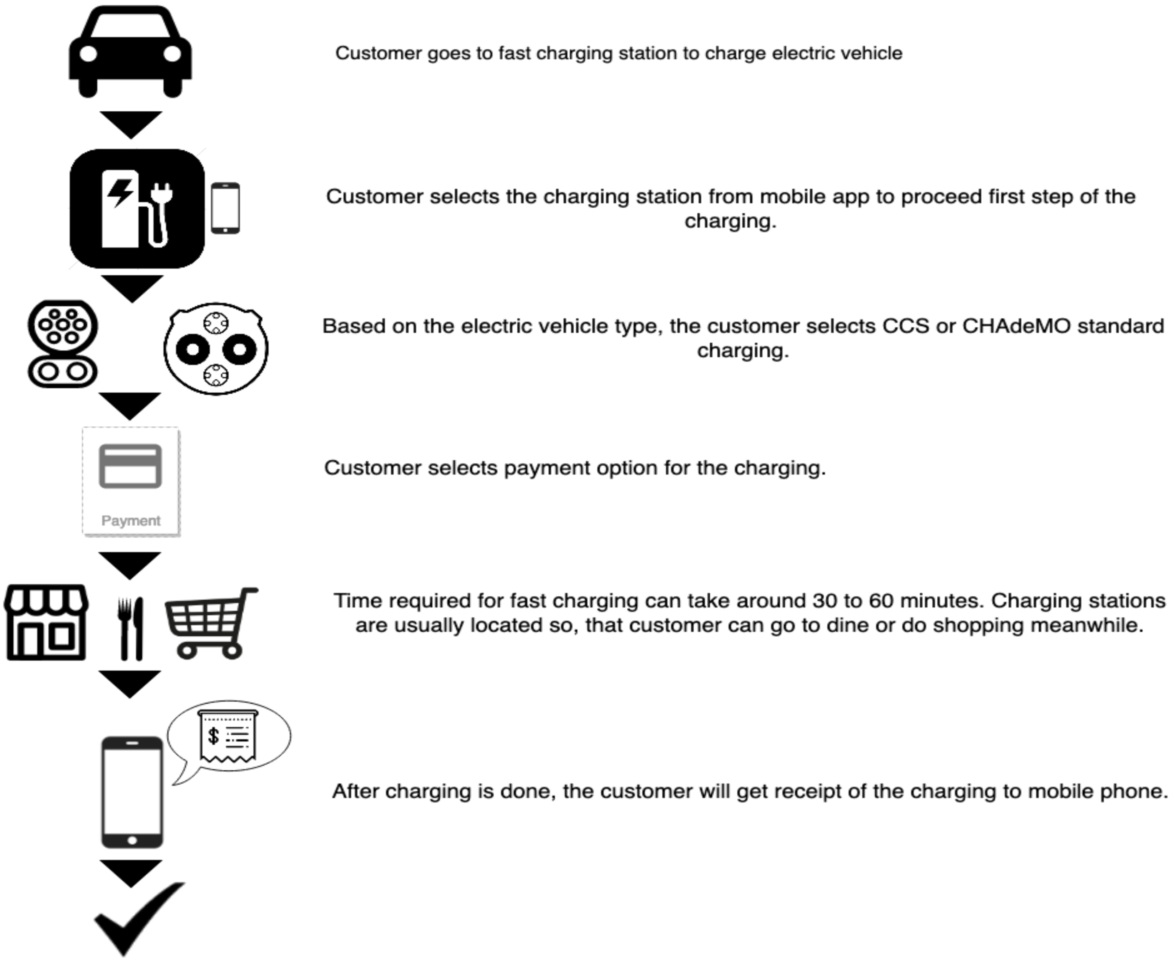
Current mobile network technology provides a powerful way to create solutions based on the existing mobile network coverage areas. With the previous chapters' information, the next chapter will go through the charging process using these technologies, equipment and tools.

8 Charging Process

The Figures shown in this chapter explain the normal human behavior when a customer needs to charge the EV. The process goes through the customer point of view of normal charging and later based on advanced charging process, which includes what kind of processes take place behind the scenes.

8.1 Normal charging process

The process of when the customer wants the EV to be charged to EV charging is completed is depicted in Figure 9.



Customer goes to fast charging station to charge electric vehicle

Customer selects the charging station from mobile app to proceed first step of the charging.

Based on the electric vehicle type, the customer selects CCS or CHAdeMO standard charging.

Customer selects payment option for the charging.

Time required for fast charging can take around 30 to 60 minutes. Charging stations are usually located so, that customer can go to dine or do shopping meanwhile.

After charging is done, the customer will get receipt of the charging to mobile phone.

Figure 9 Normal charging process from customer POV

As illustrated in Figure 9, the process has six steps. Charging time depends on the battery current battery State of Charge (SoC) as the battery could be close to full and hit the fast charging safety limit, which is roughly at 80 %. Charging stations itself are commonly owned by the retailer of their own market to attract customers to spend money meanwhile charging their EVs.

8.2 Advanced secure charging process

Following *Figure 5* shows the background activity, which keeps the *Figure 4* normal charging process running. Each process will be explained in numerical order.

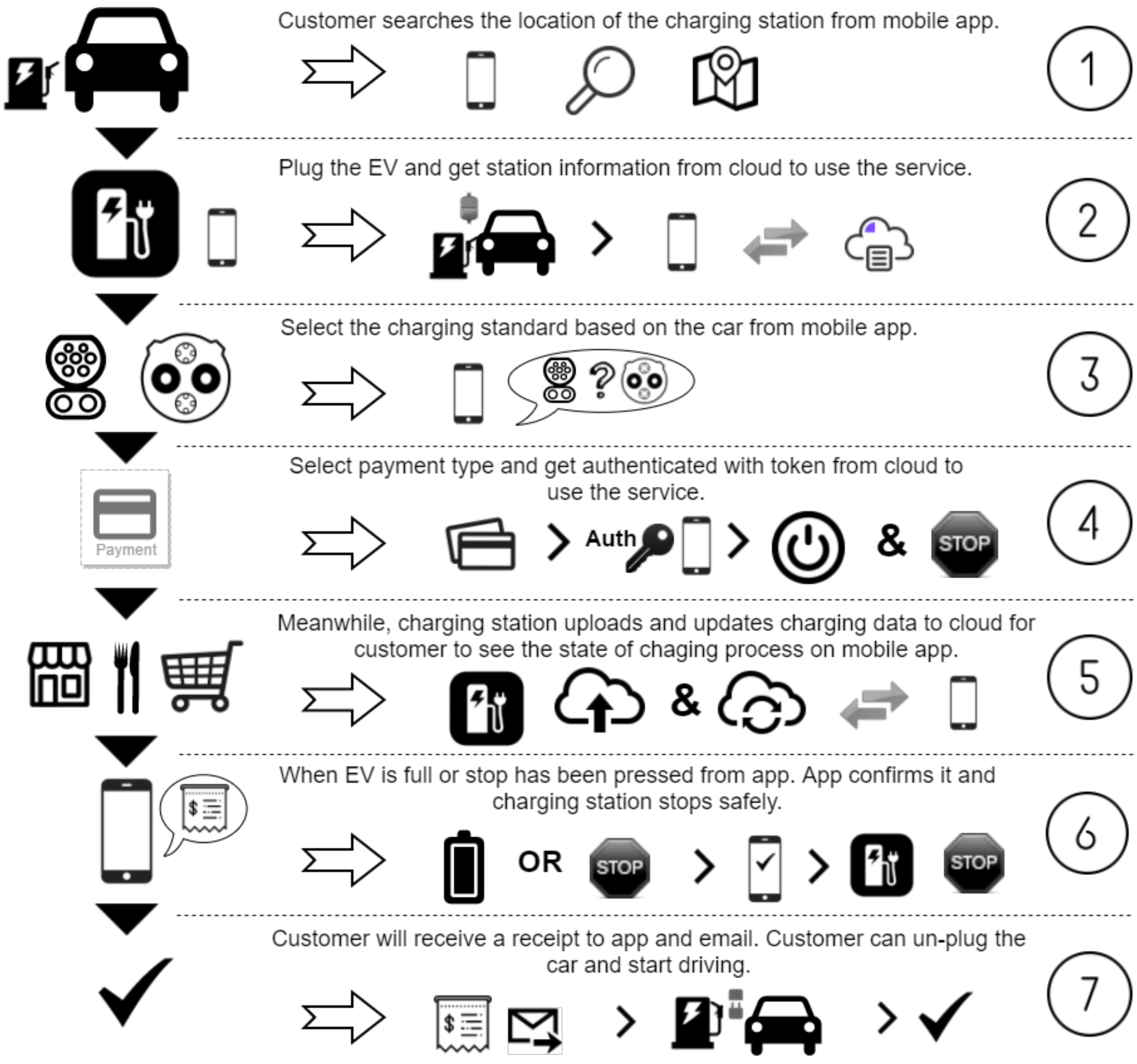

Customer searches the location of the charging station from mobile app.
1
Plug the EV and get station information from cloud to use the service.
2
Select the charging standard based on the car from mobile app.
3
Payment
Select payment type and get authenticated with token from cloud to use the service.
Auth
&
STOP
4
Meanwhile, charging station uploads and updates charging data to cloud for customer to see the state of chaging process on mobile app.
&
5
When EV is full or stop has been pressed from app. App confirms it and charging station stops safely.
OR
STOP
STOP
6
Customer will receive a receipt to app and email. Customer can un-plug the car and start driving.
7

Figure 10 Advanced charging with back-end processes

1. From mobile app front-end, the customer has a map view of charging stations and status of the stations. Charging station can be unavailable due to a problem or it can be taken by other EV. Available charging station should show the infor-

mation of its offering charging standards e.g., CHAdeMO and/or CCS. Also, location address, price per minute and power of the charging station is displayed on mobile app.

2. When available charger has been found, it can be reserved from mobile app station selection and the charging pistol can be plugged into the EV. The station recognizes the app interaction and begins to communicate next step actions through the cloud service back-end. The customer can login with own credentials or create temporary login information to get receipt of the charging.

3. Depending on the charging station, it has one or two charging connectors. In case of two connectors, the customer chooses the standard according to owner's EV. If the charging station contains each CHAdeMO and CCS standard, mobile app has option to select the desired charging standard pistol. On the other hand, if the station has both pistols with same charging standards, the app should indicate the correct one by left or right, app visualization or environment coloring.

4. Payment options are based on service provider, but supports most common credit, debit cards and PayPal, if it has been set up. Payment service provider will grant the token for the payment though tokenization procedure. With the customer's valid tokenization token, the mobile app will give access to the charging authentication token. Authentication token itself gives the customer a temporary time-based access to the start and stop actions of the app. Mobile app will send the action over API to the cloud and then customer sees updating information of the charging process.

5. The charging process normally takes approximately 10 to 40 minutes by regular basis with fast charging technology. This also depends on the battery's SoC percentage and will the car be charged all the way to 100% or till around 80%, which is still in the fast charging sweet spot before power is starting to limit the output current. The time used meanwhile charging is often used to go do business, shopping, dining and other equivalent time-consuming activities. Instead of always checking the charging station display, the information can be taken in any place with internet access and mobile phone app. Charging station updates data

in small delays to the cloud databases and forwards it to APIs. The mobile app will then read the RESTful API JSON data and update the user interface of the mobile app, thus keeping the data updated all the time.

6. When the EV has been charged to full or the customer has pressed the stop button on the mobile app, it will send the HTTP API request to cloud backend and apply the changes to the charging station controller. Controller will start lowering the voltage and the current until it unlocks the charging connector and it will be safe to remove it from the EV.

7. After charging the EV has finished, mobile app will show receipt of the charging. Receipt includes the price, kW/h and duration of the charging. Backend will take the start and stop times of the charging for bank payment and store it at least 10 years due to law regulations. Authentication token will be deleted after the charging process is completed.

Chapter 8 informed what happens during the charging from two different angles, but next chapter 9 will go into charging station’s technical side as well as protocols and standards.

9 Charging Stations

Similar to the Internal Combustion Engine (ICE) vehicles, EVs also need to fuel their cars, but with electricity. Comparing ICE vehicle and EV, the ICE vehicles have a longer range and faster to fuel gas than charge EV with electricity. Thus, along the daily driving roads need to have more EVSE on the side of the road. For this case, Direct Current Fast Charge (DCFC) EVSE are found at fuel stations, near shops and parking areas due to their faster charging time compared to Alternating Current (AC) charging. AC is mostly used overnight at home and in places where EV user is staying a longer period of time due to its limitation in charging speed. The limitation is based on EV’s on-board AC/Direct Current (DC) charger, which is not needed for DCFC charging [54].

9.1 Difference between AC and DC charging

Both charging types have their own advantages and disadvantages. The biggest advantage for the AC is the electrical grid, which is AC. Finding the AC charging is much easier because it can be attached directly to grid. Thus, it is a favorable solution at home, shopping malls and places where the EV user spends more than 20 minutes. Operation, production and installation costs are cheaper for AC chargers, which makes them more commonly seen daily charger type. DC charging shines when the EV needs to be charged faster than 30 minutes. DC charging takes advantage of directly charging the EV Li-ion battery, while AC charging needs to be converted into DC through on-board charger. *Figure 11* demonstrates the AC and DC charging.

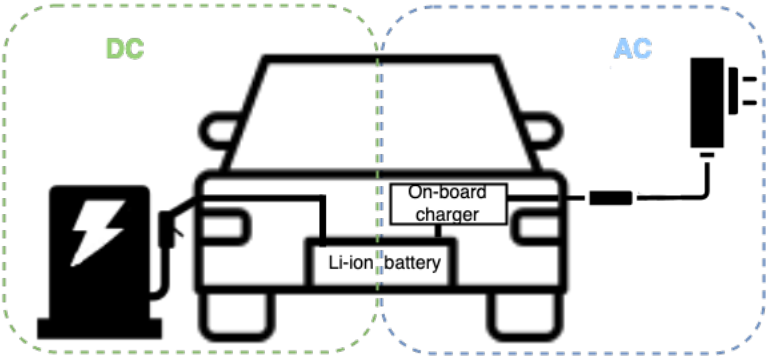


Figure 11 DC and AC charging

The charging speed itself is limited by the EV's own on-board charger, thus the high kW AC charger values are mostly showoff from manufacturers. If the EV cannot charge on high capacity due to the on-board charger, the EV user may pay high price for the amount of lower energy received. DC EVSE will do the AC/DC conversion inside its power units, thus supplies greater power to the EV. Conversion is usually done in external power unit box, except the Unified Chargers' DCFC has an all-in-one solution for that. [54][55][56].

9.2 Smart grid

Smart grid framework aims to offer a support for designing use cases with an architectural approach allowing a representation of interoperability viewpoints in a technology neutral matter. Open Charge Point Protocol (OCPP) network and Vehicle to Grid (V2G) supports EVSE communication with the EVs, which are practical with the smart grid. Both current implementation of the electrical grid and future implementations of the smart grid are used in everyday life and concerns EV's charging. The following five interoperability layers are used in framework:

- **Business Layer**. The information exchange is served on the business view. Smart grid may be used to map regulatory and market structures, business portfolios, business models and policies of market parties involved.

- **Function Layer**. Specifies services and functions including their connections from an architectural PoV. The functions are shown in systems, applications and components as separated from physical and actor implementations.

- **Information Layer**. Details the used and exchanged information between functions, components and services. Contains the underlying canonical and objects data models information. These information data models represent the approved schematics for services and functions in order to permit communication factor of an interoperable information exchange.

- **Communication Layer**. The importance of the communication layer is to detail mechanisms and protocols for the interoperable exchange of information between components. Underlying context of exchange use case in function or service and related information objects or data models.

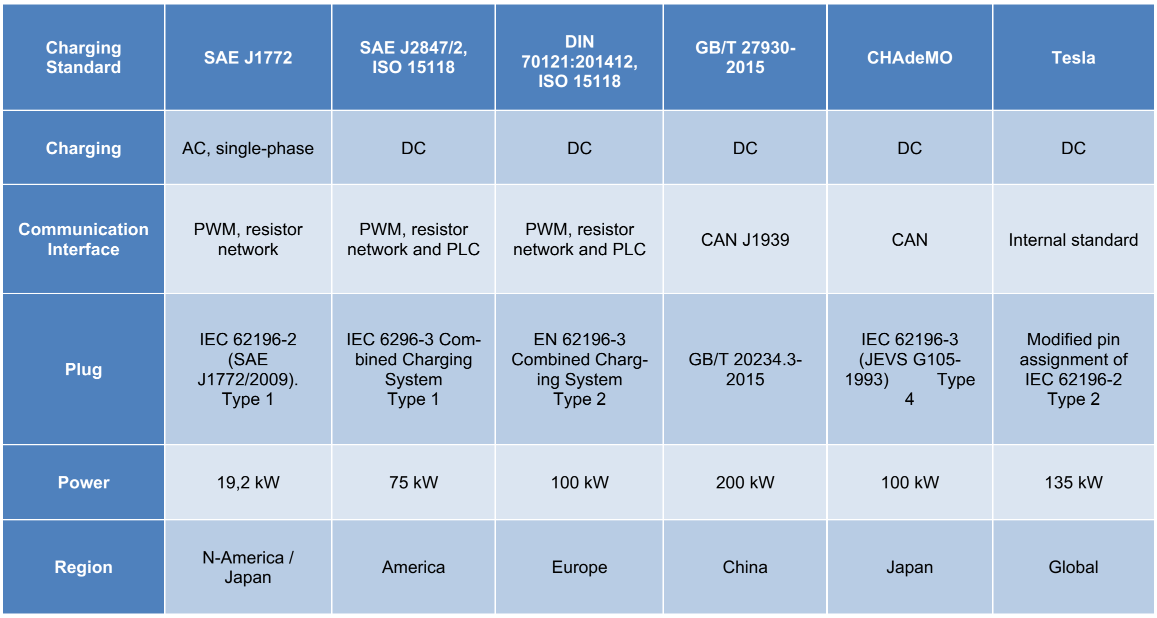
- **Component Layer**. Physical allocation of all participating components in the smart grid framework. This includes applications, power system equipment, actors, protections and tele-control devices, network infrastructure e.g. wireless/wired communication, switches, routers, servers, and any kind of computers.

Plug-and-play allows to add a new component to a system and have it working automatically without having to do any manual configuration or technical analysis. This includes the automatic configuration of specific settings necessary for system integration. Interoperability categories, the concept of automatic configurations addition standards and specifications with procedures and mechanisms to clarify system integration. Standards make installations clearer to add devices to the smart grid [57].

9.3 Charging standards

At the moment there is not a common path for charging standards as different manufacturers head their own way making EV's to specific standard. Some of the reasons, such as region's or country's power lines, frequencies or preferences are affecting the charging standards market. For example, Tesla was one of the first players in DCFC market, and they made their own charging infrastructure, standard and EV. CAN and PLC, the two communication protocols used in DCFC have small variations based on the region as well as due different manufacturers designs and electricity frequencies. China has made their own GB/T's CAN J1939 communication protocol, while mostly Japanese cars are using the CHAdeMO. CCS's PLC communication has been blooming in Europe and North-America making it more recommended and desired standard. There is a slight difference between the North-Americas 1-phase and EU's 3-phase AC charging combined with high power DC charging dedicated pins due frequency of the electricity [58][59].

More differences of the standards are shown in Figure 12 below:



Charging Standard	SAE J1772	SAE J2847/2, ISO 15118	DIN 70121:201412, ISO 15118	GB/T 27930-2015	CHAdeMO	Tesla
Charging	AC, single-phase	DC	DC	DC	DC	DC
Communication Interface	PWM, resistor network	PWM, resistor network and PLC	PWM, resistor network and PLC	CAN J1939	CAN	Internal standard
Plug	IEC 62196-2 (SAE J1772/2009). Type 1	IEC 6296-3 Combined Charging System Type 1	EN 62196-3 Combined Charging System Type 2	GB/T 20234.3-2015	IEC 62196-3 (JEVS G105-1993) Type 4	Modified pin assignment of IEC 62196-2 Type 2
Power	19,2 kW	75 kW	100 kW	200 kW	100 kW	135 kW
Region	N-America / Japan	America	Europe	China	Japan	Global

Figure 12 Charging Standards

As seen in Figure 12, plugs have 4 different types that are defined in the standards. Rapid Charge (RC) function is built combined with Type 1,2 and 3 charging.

- **Type 1**. Single-phase AC charging. Used in America and Japan.
- **Type 2**. Single/three-phase AC charging. Used in Europe.
- **Type 3**. Single/three-phase AC charging with safety shutters. EV Plug Alliance proposal.
- **Type 4**. Fast charge for CHAdeMO. Used mostly in Japan and globally [59][60].

9.3.1 CHAdeMO

CHAdeMO is one of the RC standards, which was defined by the CHAdeMO Association. The association itself was formed by the Nissan, Toyota, The Tokyo Electric Power Company, Fuji Heavy Industries and Mitsubishi. The name comes from “CHArge de MOve”. EVs require to have two charging sockets in EV as CHAdeMO does not support AC charging. The charging connector is determined by Japan Electric Vehicle Standard G105-1993. The connector itself is quite heavy and the cable is stiff to bend around. Pin layout is shown in Figure 13 below:

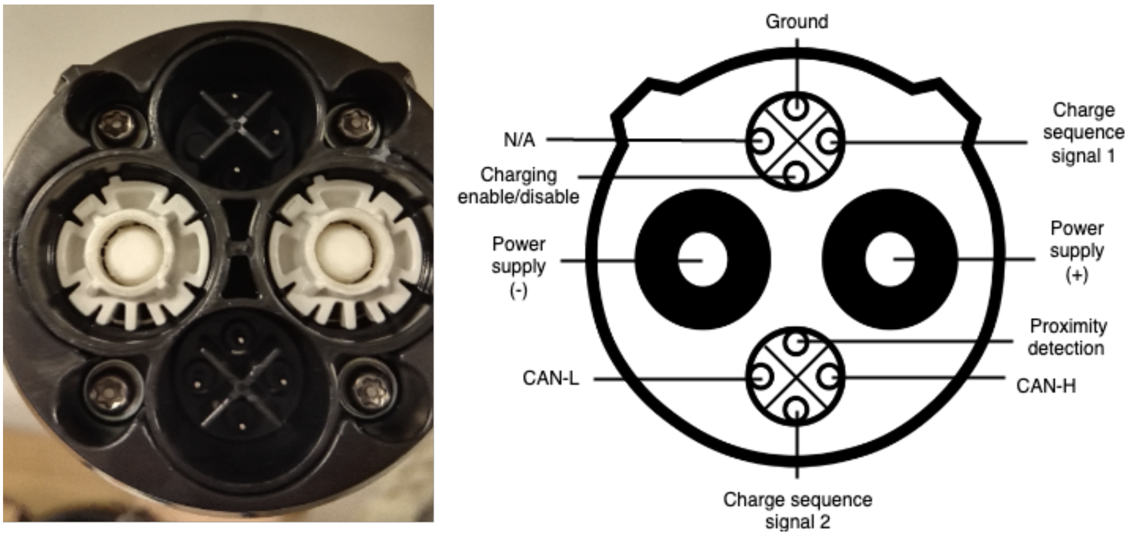


Figure 13 CHAdeMO pins

Two communication lines CAN signal and Pilot signal from the EV to EVSE are functioning as signal senders in case of malfunctioning is found on the EV side. This allows charging to stop, even when one communication line is broken. Before charging, the EV and EVSE will perform a safety test to check the circuit isolation and the short circuit of the link between. EV coupler is locked during the charging via a mechanical latch, which is locked by an electrical lock. The electrical lock will not release the connector as long there is voltage flowing. The electrical lock will release the connector from EV when charging has ended. Voltage will not drop to zero and the connector won't unlock unless it is safe to do so [61][62].

Figure 14 shows the CHAdeMO standard charging the Nissan LEAF.

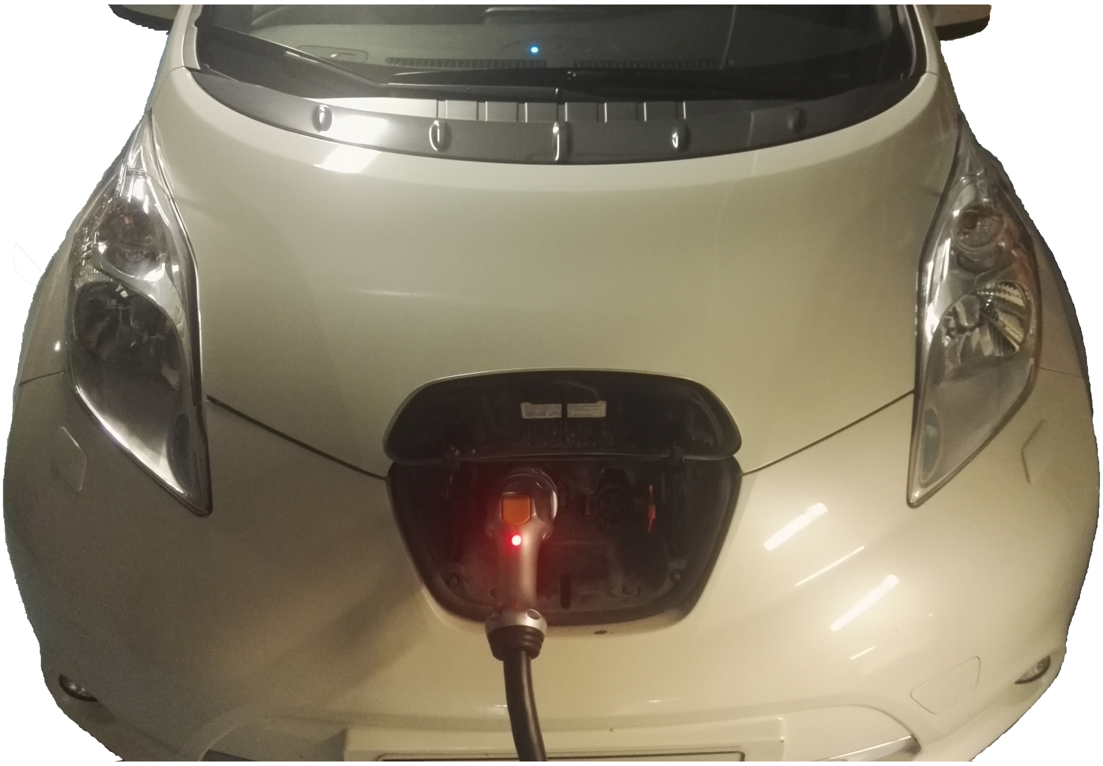


Figure 14 Nissan LEAF charging

In Figure 14, the red light on the CHAdeMO connector indicates that voltage is going through and it is electrically locked. Blue light seen through the windshield shows the battery level of the Nissan LEAF.

9.3.2 CCS

CCS uses the PLC communication, which allows Ethernet connection though the power lines. CCS is using single-phase AC in North America and almost rest of the world is using three-phase AC charging combined with Combo 1 (North-America) or Combo 2 (rest of the world) DC charging in the lower part of the connector (*Figure 15*). Compared to CHAdeMO, CCS allows AC charging in the same inlet [58][59].

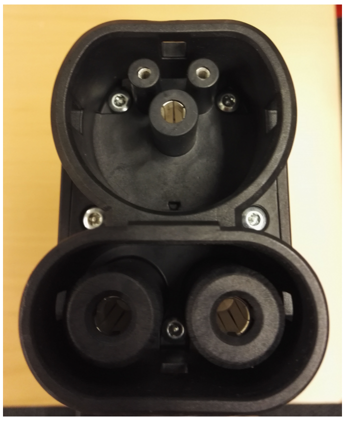


Figure 15 CCS Combo connector

The CCS connector has pins for Control Pilot (CP), Proximity Pilot (PP), Protective Earth (PE), N, L1, L2 and L3.

9.3.3 Wireless charging

Wirelessly charging mobile phones have been in use for a while now, which could be the future for EV's as well. The Society of Automotive Engineers (SAE) has been working with a set of global standards to make wireless charging possible via different wireless systems. Wireless charging is still maturing to become a daily charging option, but the engineers are working hard to make it part of the EV charging ecosystem. Charging occurs in a magnetic resonance process and the charging itself proceeds when the car parks on top of the wireless charger. The method would be ideal in e.g. tight parking halls where time spent is the same as AC charging and space is limited for EVSE [63].

10 Findings and Conclusions

The purpose of this thesis project was to research the possibility to create an Internet of Things (IoT) solution for a fast charging station, which would be compact and smart for commercial and private usage. The project itself progressed so that a real EV was tested and charged.

The findings of this study showed that it is possible to find a way to update data to user without needing the charging station display and the unsecure RFID tags. Also, the Cloud can be used to provide extra freedom to work with.

Some data transfer protocols have not been efficient enough to keep updates rolling in real-time and start adding small delays overtime, which will lead into bigger problems later. For example, some time-based crucial data needs to be updated based on standard milliseconds and if it adds delay, then it will cause a problem and the whole protocol will go down.

3G network public IP addresses are blocked by the operator’s NAT by default. Some providers will charge extra to allow the SIM card to have a public IP.

Radio-Frequency Identification (RFID) cards are a security risk for charging stations and their users. Cards can be reverse engineered or eavesdropped by capturing the radio frequency waves from the use case. This can be used to whitelist unauthorized personnel or even steal the card user authorization and charge the user.

The future will show the sunny side for the EV ecosystem and more innovative and secure EVSEs are going to be needed for commercial and industrial usage. Services are moving to mobile, which is logical to follow the trend in EVSE development and use the modern technology to ensure it’s updated. Lots of engineering still needs to be done to make EVs and EVSEs more available and affordable around the globe. Cloud is a good source for making things such as IoT available more broadly.

Personally, I learned much more than I thought during this thesis project, even though it felt quite overwhelming at the beginning to touch a subject, about which I didn’t have experience. But I am glad that I did.

References

1 Nuccitelli, Dana. 2018. Switching to electric cats is key to fixing America’s ‘critically insufficent’ climate policies. The Guardian. <https://www.theguardian.com/environment/climate-consensus-97-per-cent/2018/jan/22/switching-to-electric-cars-is-key-to-fixing-americas-critically-insufficient-climate-policies>. Read 20.October.2018.

2 Kane, Mark. 2018. Over 50 Plug-In EVs Compared: Price, Range + More – May 2018. InsideEVs. <https://insideevs.com/over-50-plug-in-evs-compared-price-range-more-march-2018-us/>. Updated 17.September.2018. Read 20.October.2018.

3 American Automobile Engineers. 2019. AAA Electric Vehicle range testing. <https://www.aaa.com/AAA/common/AAR/files/AAA-Electric-Vehicle-Range-Testing-Report.pdf>. Read 2.April.2019.

4 Marshall, Brian. 2002. How Electric Cars Work. <https://auto.howstuffworks.com/electric-car.htm>. Read 8.April.2019.

5 Alternative Fuels Data Center. How Do All-Electric Cars Work? <https://afdc.energy.gov/vehicles/how-do-all-electric-cars-work>. Read 8.April.2019.

6 Union of Concerned Scientists. 2015. How Do Battery Electric Cars Work? <https://www.ucsusa.org/clean-vehicles/electric-vehicles/how-do-battery-electric-cars-work>. Updated 12.March.2018. Read 8.April.2019.

7 Car Keys. 2018. Guide to the different types of electric vehicles. <https://www.carkeys.co.uk/guides/guide-to-the-different-types-of-electric-vehicles>. Read 8.April.2019.

8 Union of Concerned Scientis. 2016. What is ZEV? <https://www.ucsusa.org/clean-vehicles/california-and-western-states/what-is-zev>. Updated 31.October.2016. Read 8.April.2019.

9 Fielding, Roy Thomas. 2000. Architectural Styles and the Design of Network-based Software Architectures. Doctor of Philosophy in Information and Computer Science. University of California, Irvine. <https://www.ics.uci.edu/~fielding/pubs/dissertation/fielding_dissertation.pdf>.

10 JSONAPI Documentation. <https://jsonapi.org/format/>. Read 23.October.2018.

11 Design by Matias Mäenpää. Unified Chargers charging station. <http://www.unifiedchargers.fi/> Visited 15.October.2018.

12 Unified Chargers Ltd. Home page. <http://www.unifiedchargers.fi/> Read 18.October.2018.

13 Hale, Zach. 2018. Cloud ERP vs On-Premise ERP. <https://www.softwareadvice.com/resources/cloud-erp-vs-on-premise/>. Read 25.October.2018.

14 Grispos, G., Glisson, W.B., and Storer, T. 2013. Cloud Security Challenges: Investigating Policies, Standards, and Guidelines in a Fortune 500 Organization. In: 21st European Conference on Information Systems, 5 - 8 Jun 2013, Utrecht, The Netherlands. pp.2-4

15 Johnson, Pete. 2017. Is 7-Layer OSI Still Relevant in a Cloud World? <https://www.cbronline.com/in-depth/7-layer-osi-still-relevant-cloud-world>. Read 25.October.2018.

16 Arista. 2013. Security for the Cloud Data Center. <https://www.arista.com/assets/data/pdf/Whitepapers/ARISTA_SecuritySolutionWP.pdf>. Read 25. October.2018.

17 Oestreich, Ken. 2010. Converged Infrastructure. <https://web.archive.org/web/20120113094920/http://www.thectoforum.com/content/converged-infrastructure-0>. 13.January.2012.

18 Mell, Peter and Grance, Timothy. 2011. National Institute of Standards and Technology. The NIST Definition of Cloud Computing. pp.2-3.

19 Henderson, Amy. 2018. Secure Data Centers: When the Best Advice is to Get the Best Advice. <https://blogs.cisco.com/security/secure-data-centers-when-the-best-advice-is-to-get-the-best-advice>. Read 8.March.2019

20 Microsoft. What is IaaS? <https://azure.microsoft.com/en-us/overview/what-is-iaas/>. Read 8.March.2019.

21 Microsoft. What is PaaS? <https://azure.microsoft.com/en-us/overview/what-is-paas/>. Read 8.March.2019.

22 Hurwitz, J., Kaufman, M., Halper, F. and Kirsch, D. 2012. <https://www.dummies.com/programming/cloud-computing/hybrid-cloud/the-business-benefits-of-paas-in-cloud-computing/>. Read 8.March.2019.

23 Microsoft. What is SaaS? <https://azure.microsoft.com/en-us/overview/what-is-saas/>. Read 8.March.2019

24 Set a Time Blog. 2018. What is Software as a Service (SaaS)? – Simplified. <https://setatime.co/blog/what-is-software-as-a-service-saas-simplified/>. Updated 31.December.2018. Read 8.March.2019.

25 Hille, M., Klemm, D. and Lemmermann, L. 2017. Crisp Research. Cloud Computing Vendor & Service Provider comparison. <https://www.reply.com/Documents/Crisp_Vendor_Universe_Cloud%20Computing_250118_REPLY_englisch-eVersion_FINAL.pdf>. pp. 6-7. Read 13.March.2019.

26 CloudCodes. 2018. Understanding Fault Tolerance in Cloud Computing and Its Significance. <https://cloudcodes.com/blog/fault-tolerance-in-cloud-computing.html>. Read 13.March.2019.

27 MQTT. MQQT FAQ. <https://mqtt.org/faq>. Read 23.October.2018.

28 Imperva. 2015. Man in the Cloud (MITC) Attacks. <https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf>. Read 25.March.2019.

29 Ajey Singh, Dr. Maneesh Shrivastava. 2012. Overview of Attacks on Cloud Computing. <http://www.ijeit.com/vol%201/Issue%204/IJEIT1412201204_57.pdf>. pp. 321-323. Read 25.March.2019.

30 Redhat. What is different about cloud security. <https://www.redhat.com/en/topics/security/cloud-security>. Read 25.March.2019.

31 Amazon Web Services. The Beginner's Guide to Cloud Security. <https://aws.amazon.com/security/introduction-to-cloud-security/>. Read 25.March.2019.

32 IBM. 2018. Public clouds, private clouds and your security. <https://www.ibm.com/ibm/files/Z702257B23536P19/15PPCLOUDCOMPUTING_116KB.pdf>. Read 25.March.2019.

33 Martins, Flavio. 2014. 3 Quick Facts on Why a Strong Password Policy Matters. <https://www.digicert.com/blog/3-reasons-for-strong-password-policy/>. Read 25.March.2019.

34 Cloud Security Alliance. 2011. Defined Categories of Service 2011. <https://cloudsecurityalliance.org/wp-uploads/2011/09/SecaaS_V1_0.pdf>. Read 25.March.2019.

35 Tyson, Jeff and Crawford, Stephanie. How VPNs Work. <https://computer.howstuffworks.com/vpn7.htm>. Read 25.March.2019.

36 Morgan, Jacob. 2014. A Simple Explanation Of 'The Internet Of Things'. <https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#344d55291d09>. Read 26.March.2019.

37 Patterson, S. M. 2017. 5 reasons why device makers cannot secure the IoT platform. <https://www.networkworld.com/article/3223952/5-reasons-why-device-makers-cannot-secure-the-iot-platform.html>. Read 26.March.2019.

38 Smith, George. 2017. Clarifying IoT and M2M. <https://dzone.com/articles/clarifying-iot-and-m2m>. Read 26.March.2019.

39 Emqqt. 2017. MQTT in a Nutshell. <https://medium.com/@emqtt/mqtt-in-a-nutshell-cc24370920c2>. Read 26.March.2019.

40 Gupta, Rahul. 2014. 5 Things to Know About MQTT – The Protocol for Internet of Things. <https://www.ibm.com/developerworks/community/blogs/5things/entry/5_things_to_know_about_mqtt_the_protocol_for_internet_of_things?lang=en>. Read 26.March.2019.

41 Eclipse. 2018. Quality of service. <https://www.eclipse.org/paho/files/mqttdoc/MQTTClient/html/qos.html>. Read 26.March.2019.

42 Pacheco, Jesus and Hariri, Salim. 2016. IoT Security Framework for Smart Cyber Infrastructures. pp. 242-244. Read 27.March.2019.

43 NCCIC. 2009. Understanding Denial-of-Service Attacks. <https://www.us-cert.gov/ncas/tips/ST04-015>. Last revised 28.June.2018. Read 27.March.2019.

44 ENISA. 2017. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. Read 1.April.2019.

45 HiveMQ. MQTT Security Fundamentals. <https://www.hivemq.com/blog/mqtt-security-fundamentals-tls-ssl>. Read 23.October.2018.

46 Bahia, Kalvin. 2018. State of Mobile Internet Connectivity 2018. <https://www.gsmaintelligence.com/research/?file=c0bcc185be555f77478a8fdf986ea318&download>. Read 29.March.2019.

47 WorldTimeZone. GSM Bands information by country. <https://www.worldtimezone.com/gsm.html>. Updated February.2019. Read 29.March.2019

48 Simpson, William Allen. 1994. The Point-to-Point Protocol (PPP). <https://tools.ietf.org/html/rfc1661>. Updated May.1997. Read 29.March.2019.

49 Whatismyipaddress. What is PPP and PPPoE? <https://whatismyipaddress.com/ppp-pppoe>. Read 29.March.2019.

50 Proxicast. 2012. How does the CSQ value relate to RSSI? <http://www.proxicast.com/AbsoluteFM/afmviewfaq.aspx?faqid=36>. Read 1.April.2019

51 Wang, Ershen; Zhang, Shufang and Zhang Zhixian. 2012. Research and Implement of PPP and TCP/IP Protocol based on GPRS. pp 1-4. Read 1.April.2019.

52 Adrian. 2016. Conversion of signal strength in dBm to percentage in WiFi Explorer. <https://www.adriangranados.com/blog/dbm-to-percent-conversion>. Read 1.April.2019.

53 M2MSupport. 2012. ATCSQ signal quality. <https://m2msupport.net/m2msupport/atcsq-signal-quality/>. Updated 9.December.2018. Read 1.April.2019.

54 Newmotion. AC Charging vs DC Charging. <https://newmotion.com/ac-charging-vs-dc-charging>. Read 3.April.2019.

55 EV Safe Charge. DC Fast Charging Explained. <https://evsafecharge.com/dc-fast-charging-explained/>. Read 4.April.2019.

56 Schwitters, Chad. 2013. AC versus DC charging – what is the difference. <https://pluginamerica.org/ac-versus-dc-charging-what-difference/>. Read 4.April.2019.

57 GEN-CENELEC-ETSI Smart Grid Coordination Group. Smart Grid Reference Architecture. Pp. 15, 27 and 61.

58 Kane, Mark. 2018. European CCS (Type 2 / Combo) Conquers World – CCS Combo 1 Exclusive To North America. <https://insideevs.com/european-ccs-type-2-combo-2-conqueres-the-world/>. Read 5.April.2019.

59 Aaltonen, Topi. Types of charging plugs for electric vehicles. <https://plugit.fi/en-gb/article/etusivu/types-of-charging-plugs-for-electric-vehicles/135/>. Read 5.April.2019.

60 Wikipedia. Charging station. <https://en.wikipedia.org/wiki/Charging_station>. Read 5.April.2019.

61 Herron, David. 2017. EV DC Fast Charging standards – CHAdeMO, CCS, SAE Combo, Tesla Supercharger, etc. <https://greentransportation.info/ev-charging/range-confidence/chap8-tech/ev-dc-fast-charging-standards-chademo-ccs-sae-combo-tesla-supercharger-etc.html>. Read 7.April.2019.

62 CHAdeMO. Technology overview. <https://www.chademo.com/technology/technology-overview/>. Read 7.April.2019.

63 Hurst, Nathan. 2018. Is Wireless Charging for Cars Finally Here? <https://www.smithsonianmag.com/innovation/wireless-charging-cars-finally-here-180970494/>. Read 8.April.2019.

3G Network related measurements

Value (CSQ)	RSSI dBm	Condition
99,99		No Signal
2	-109	Marginal
3	-107	Marginal
4	-105	Marginal
5	-103	Marginal
6	-101	Marginal
7	-99	Marginal
8	-97	Marginal
9	-95	Marginal
10	-93	OK
11	-91	OK
12	-89	OK
13	-87	OK
14	-85	OK
15	-83	Good
16	-81	Good
17	-79	Good
18	-77	Good
19	-75	Good
20	-73	Excellent
22	-69	Excellent
24	-65	Excellent
26	-61	Excellent
28	-57	Excellent
30	-53	Excellent

Test +CSQ	RSSI dBm	Condition
3,99	-107	Marginal
2,99	-109	Marginal
3,99	-107	Marginal
3,99	-107	Marginal
2,99	-109	Marginal
3,99	-107	Marginal
4,99	-105	Marginal
3,99	-107	Marginal
2,99	-109	Marginal
99,99	none	No Signal
2,99	-109	Marginal
3,99	-107	Marginal
3,99	-107	Marginal
4,99	-105	Marginal
8,99	-97	Marginal
7,99	-99	Marginal
7,99	-99	Marginal
7,99	-99	Marginal
7,99	-99	Marginal
11,99	-91	OK
0,99	-113	Marginal
6,99	-101	Marginal

Value (CSQ)	RSSI dBm	Condition
99,99		No Signal
2	-109	Marginal
9	-95	Marginal
10	-93	OK
14	-85	OK

15	-83	Good
19	-75	Good
20	-73	Excellent
30	-53	Excellent