Billing Infrastructure for a Charging System for E-Cars

Orlin Tomov

Abstract: *The paper is focused on the development of a universal WEB-based billing system, for the needs of a charging infrastructure for e-cars. The system uses RFID cards for client identification and provides basic cashier functionalities. Some of the security aspects are also described in the article.*

Key words: *WEB-based information system, Billing system, WEB security.*

INTRODUCTION

At the moment there are more than 12 companies at the market, offering electric cars [1]. Their popularisation is tightly related and dependent from the charging infrastructure. Normally such a vehicle can be charged, using a normal electrical outlet. The main problem is, that the charging process is relatively slow, and the mileage is not very high. Due to these disadvantages, in order to use any electric powered vehicle, it should be charged at any possibility. That's why the need of a wide-spread charging infrastructure is necessary.

The modern concept for the charging station is a fully automatic “box”, with a friendly users' interface and requiring no staff to operate. To achieve this functionality, a background information system should be used. It provides the correct information transmission and storage for every action on each charging station or cash point.

A CONCEPT FOR THE CHARGING STATION

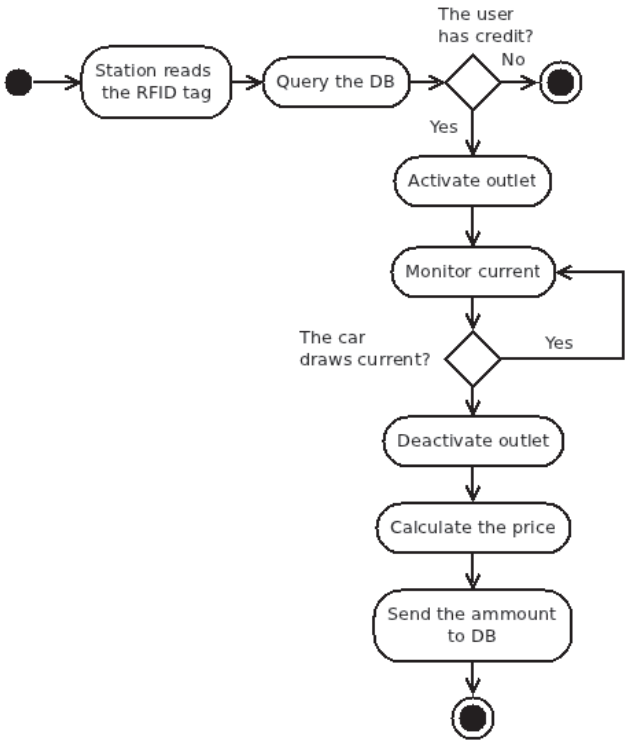

Fig. 1 – A basic concept for the functionality of the charging station

The concept (fig. 1, 2, 3) is focused on the staff-less operation of every charging "box". To provide the payment for the consumed energy, each user should have a personal RFID card to identify himself in front of the information system. These cards have to be pre-paid on a cash-desks, which could be in the supermarkets for example. After user identification, the charging station queries the database for the RFID tag. If the credit is enough to perform a charge, the power outlet is being activated and the user is informed. After the process is finished (no current is drawn from the outlet), the station sends a query to the database server for recording the details of the process.

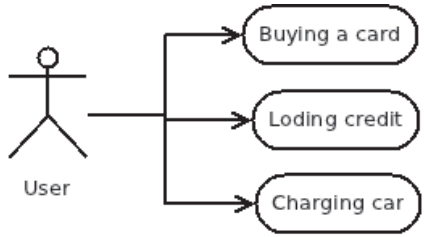

Fig. 2 – User's activity

On figures 2, 5 and 4 are shown the activity diagrams for the different agents – user, cashier and administrator.

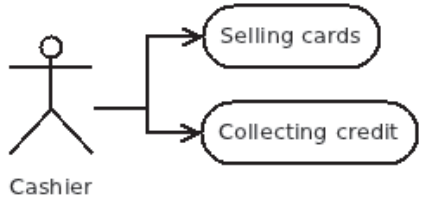

Fig. 3 – Cashier's activity

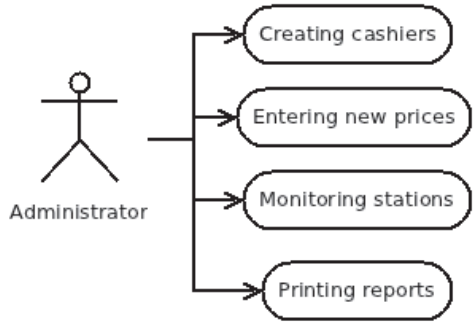

Fig. 4 – Administrator's activity

IMPLEMENTATION OF SECURE DATA TRANSMISSION

Since the need of as much of possible charging points, their interconnection, using wire lines is very expensive for implementing. That's why our data transmission is based on GPRS traffic over the existing GSM infrastructure. So every “box” is equipped with a GSM/GPRS modem. The communication diagram is shown on fig. 5.

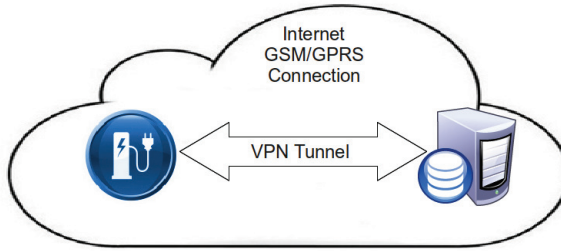

Fig. 5 – Connection between the charging box and DB server

Each charging station is equipped GSM/GPRS modem. The link with the database server is accomplished via encrypted VPN tunnel [4] (fig. 5).

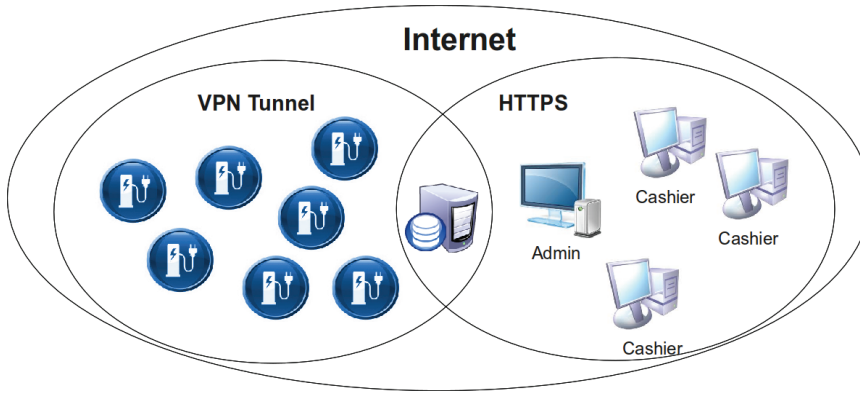

Fig. 6 – Connection between all the agents in the system

The connection between administrator and cashiers on one hand and the database server on another is based on HTTPS protocol and for the encryption are used client side certificates on smartcards. Using this technology it is guaranteed, that unauthorised access will be restricted.

IMPLEMENTATION OF SECURE DATA STORAGE

Special precautions has been taken for the data security on the database server. The data is responsible and sensitive from physical and logical failure of the system. That's why data safety has a primary importance.

Logically, as shown on figure 6., there is only one server. Physically, the servers are two and they work in a cluster, managed by the heartbeat system and DRBD. The two machines have identical software products installed. Each of them is equipped with 2 SSD hard drives, working in RAID 1 mode. This provides the stability and data integrity in each physical machine. The disk arrays are interconnected with the DRBD system which synchronises the both arrays in real time, using the internal network.

The organisation of the servers is master-slave. The heartbeat system of the slave machine is testing the services of the master. If the master machine stops responding, then the slave assigns the IP address of the master and fires up the DBMS and WEB server.

CONCLUSIONS AND FUTURE WORK

This is the very first configuration of the system and it is in test period. Currently the system is being cleared from bugs. A new e-mail messaging system should be installed in order to inform the system administrator when failure occurs.

REFERENCES

[1] http://en.wikipedia.org/wiki/Electric_car

[2] Kai Hwang, Orthogonal striping and mirroring in distributed RAID for I/O-centric cluster computing,, IEEE Transactions on Parallel and Distributed Systems, vol. 13, 2002, p.26-44

[3] A Langley, Opportunistic encryption everywhere, Web 2.0 Security & Privacy 2009, http://www.w2spconf.com/2009/

[4] C. Schmeing. (2004, March) FreeS/WAN announcement. http://www.freeswan.org/ending letter.html

Contact information:

assist. prof. Orlin Tomov, PhD, Department of Computer Systems, University of Rousse, Phone: +359 82 888 276, E-mail: OTomov@ecs.uni-ruse.bg

The paper has been reviewed.