Risk Analysis of the Cloud Infrastructure of Smart Grid and Internet of Things

Katrin Neubauer
Dept. Computer Science and Mathematics
Ostbayerische Technische Hochschule
Regensburg, Germany
email:
katrin1.neubauer@oth-regensburg.de

Sebastian Fischer
Secure Systems Engineering
Fraunhofer AISEC
Berlin, Germany
email:
sebastian.fischer@aisec.fraunhofer.de

Rudolf Hackenberg
Dept. Computer Science and Mathematics
Ostbayerische Technische Hochschule
Regensburg, Germany
email:
rudolf.hackenberg@oth-regensburg.de

***Abstract*—Cloud Computing (CC), Internet of Thing (IoT) and Smart Grid (SG) are separate technologies. The digital transformation of the energy industry and the increasing digitalization in the private sector connect these technologies. At the moment, CC is used as a service provider for IoT. Currently in Germany, the SG is under construction and a cloud connection to the infrastructure has not been implemented yet. To build the SG cloud, the new laws for privacy must be implemented and therefore it's important to know which data can be stored and distributed over a cloud. In order to be able to use future innovative services, SG and IoT must be combined. For this, in the next step we connect the SG infrastructure with the IoT. A potential insecure device and network (IoT) should be able to transfer data to and from a critical infrastructure (SG). In detail, we focus on two different connections: the communication between the smart meter switching box and the IoT device and the data transferred between the IoT and SG cloud. In our example, a connected charging station with cloud services is connected with a SG infrastructure. To create a really smart service, the charging station needs a connection to the SG to get the current amount of renewable energy in the grid. Private data, such as name, address and payment details, should not be transferred to the IoT cloud. With these two connections, new threads emerge. In this case, availability, confidentiality and integrity must be ensured. A risk analysis over all the cloud connections, including the vulnerability and the ability of an attacker and the resulting risk are developed in this paper.**

Keywords*—*Smart Grid; Internet of Things; security analysis; safety-critical infrastructure; cloud computing

I. Introduction

The increasing use of digital systems is changing our world. This development is driven among other things by Internet of Things (IoT), Smart Grid (SG) and Cloud Computing (CC) technology. IoT, SG and Cloud are separate technologies. The digital transformation of the energy industry and the increasing digitalization in the private sector, connect these technologies. Future SG are highly networked systems. In order to be able to use future innovative services, IoT, SG and CC must be joined.

The integration of SG (intelligent energy supply system) is creating a new IT infrastructure in Germany for the transmission of data. For smart metering, an intelligent measuring system (iMSys) will be integrated in the future. The iMSys consists of a basic meter (smart meter) and the smart meter gateway (SMGW) [1]. The changeover is not only taking place in Germany, but also in other European countries. The pioneers are countries like Italy or Sweden. However, these roll-outs highlight the risks with regard to safety and security. Attacks on power grid control system via the internet represent a growing threat.

The increasing digitalization and networking of all kind of devices (charging station, sensors, household appliances, etc.) is known as IoT. The devices get a communication interface and are connected to the internet (directly or via a gateway). This increasing networking of different devices creates new challenges, like scalability. A service which until now had to manage only a few devices gets new users on a large scale. These new users are not always available or disappear just as quickly. It must be possible to react flexibly to this volatility.

Smart services are required for future application “SG and IoT”. Cloud platforms are needed to use these services. The cloud platform can be described as a data hub. In this case, we have two cloud platforms. The IoT cloud from the IoT infrastructure and Smart Grid cloud (SG cloud) are used for data storage, analysis and new services.

In order to develop new innovative services in SG, such as value-added service, IoT, SG and must be combined. For this, we connect the SG infrastructure with the IoT. A potential insecure device and network (IoT) should be able to transfer data to and from a critical infrastructure (SG). By connecting the systems, new risks and attack vectors arise. These influence the security objectives - availability, confidentiality, integrity and, additional, privacy. In this case, more and more data is generated and more data accesses take place. This leads to new requirements for authentication and authorization.

This paper will explore the problems that arise in the networking of IoT, SG and CC. The aim is to identify new threats and problems and additional define technical and organizational requirements for future systems. The paper is structured as follows. Section II describes the related work. Section III introduces our architecture, while Section IV analyzes the security, followed by a conclusion in Section VI.

II. Related Work

IoT devices can be protected with known principles, but they also have to be implemented by the manufacturers. According to the current state, the most frequent security gaps can be closed with already known methods. It is important for research to respond to new challenges.

The first challenge is the scarce resources of IoT devices. Already known encryption algorithms need to be adapted or changed to work more effectively and operate acceptably with low-performance hardware (e.g. PRINCE [2]). Another possibility is to redevelop suitable algorithms (e.g. Secure IoT - SIT [3]).

At the moment, insecure devices are in use and therefore, solutions must be found to continue the operation. For example, several companies (including IBM) have developed a special DNS server (Quad9 DNS Privacy and Security Service), which should ensure the security as well as privacy of the IoT devices. Quad9 automatically blocks requests to infected sites. As a last challenge, manufacturers must be "forced" to improve IT security. This can be accomplished by guidelines and certifications.

The Smart Grid Architecture Model (SGAM) is a European architecture model that was developed in the context of the European standardization mandate M/490. It serves for the visualization, validation and structuring of SG projects from the beginning of the project as well as for the standardization of SG. In general, it is used for architecture development in the SG at different organizational levels. In this context, security is regarded as a cross-cutting topic and is not explicitly considered [4]. An analysis of the architecture in the SG shows that the architectural models of the countries differ in principle. The architecture models are mostly based on the SGAM. In Germany, the SG itself is regulated by the specifications of the Federal Office for Information Security (BSI) and is regarded as the state of the art (communication) [5]. The BSI was commissioned by the legislator to develop specifications for a SMGW in order to guarantee a secure infrastructure for intelligent measuring systems [6]. The intelligent measuring systems will be integrated into a communication network. The central element is the smart meter gateway as a communication unit [16]–[18]. In [14] and [15], there are the security and privacy considerations for IoT application on SG with a focus on survey and research challenges presented. It gives an overview about SG and IoT application on SG and identifies some of the remaining challenges and vulnerabilities related to security and privacy.

There are several publications [20]–[22] covering the subject security and privacy in SG and cloud applications. The focus of this publication is additionally the security and communication analysis of SG, IoT and CC in Germany.

Open questions with no related work, not exclusively in the scientific community, are the handling of data when they leave the "SG", requirements for authentication and authorisation in future SG-IoT-cloud application and how to deal with service provider who access data (service charging station) in critical infrastructures.

III. Architecture Challenges for Smart Grid and IoT

The SG reference architecture consist of the Local Metrological Network (LMN), the Wide Area Network (WAN) and the Home Area Network (HAN). The communication takes place through the SMGW. The SG infrastructure is extended with a SG cloud. This SG cloud enables additionally application for smart metering. For new applications and services, the existing architecture is extended with IoT devices. The IoT architecture consists of a device or sensor, connected via gateway to the router and the IoT cloud. The collected data is stored centrally on a server. This data is available to the user if rhequired. Figure 1 shows the unification of the architecture the cloud application on SG and IoT.

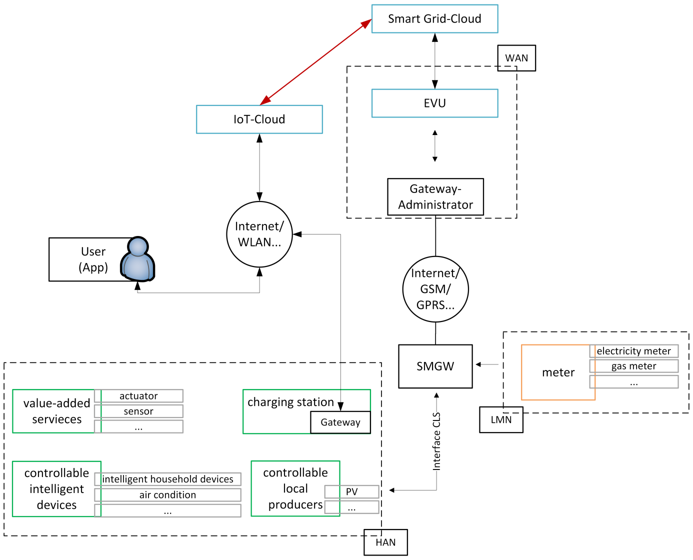

Figure 1. Architecture Cloud Application on Smart Grid with IoT

A. Application Example

In our example, a charging station with an IoT cloud is connected to a smart home. The home includes a smart meter, which is connected to the SG infrastructure and the corresponding SG cloud (Figure 1). To create a really smart service, the charging station needs a connection to the SG to get the current amount of renewable energy in the grid. This enables the possibility to load the car at the best times and supply the grid with stored energy from the car to stabilize it. The easiest way of getting these information is by connecting the two clouds (e.g. using predefined APIs).

B. Communication between Smart Grid and IoT

For a more detailed analysis, it is important to know, which data is stored on the IoT cloud and the SG cloud. In chapter "IV-C Communication between devices" this information is used to determine the risks of the communication between the two clouds.

1) Communications data Internet of Thing: The following data is stored in the IoT cloud:

- Connected car
- Sum of energy consumption
- Current energy consumption / supply
- History of energy consumption / supply
- Time to load the car
- User Data
  - Name
  - E-Mail

The connected car and the history can be used to create a profile of the user. This includes the times, the user is normally at home or at work. This data is private data and should be protected.

2) Communications data Smart Grid: The following data is generated and stored in the SG cloud:

- Information about the smart meter (ID, IP-Address)
- Current energy consumption
- Current price for electricity
- Information about the customer
  - Name
  - Address
  - Payment details

The information about the smart meter or the current energy consumption can be used to create a profile of the household (user). This is partly equal to the profile of the connected car, but can be extended to the whole household an therefore other people. In conclusion, like the connected car data, this data is also private data and should be protected.

IV. Security Analysis for Safety-critical Systems

The security analysis starts with the description of the attack vectors. From these vectors, the threads are derived. In the next step, the risk is shown for every thread, based on the ability of the attacker and the possible damage. Finally, two practical examples show the potential danger in our example architecture.

A. Attack vector Smart Grid and Internet of Thing

New attack vectors are emerging as a result of increasing networks (e.g. IoT and SG). IoT devices are potentially insecure. An attack is an unauthorized attempt to gain access [7]. If we analyze the previously described architecture with regard to potential attacks that influences the target of authenticity, current threats and gaps arise. Inspired by Hutle, the attack vector can be divided into the following categories (cf. Sichler 2014 [8] and Babar 2010 [9]).

1) Hardware manipulation attacks (physical attacks): With physical access to the device, the hardware and software can be changed. Malware installation is likely, which can lead to data manipulation and modification. At worst, a shutdown of the energy grid is possible or sensitive data (from the IoT cloud or SG cloud) can be manipulate. Furthermore, it is possible that, e.g. IoT services (IoT cloud), fail.

2) Software manipulation attacks: With integration of malware (on embedded software) or exploiting vulnerabilities (for example buffer overflow, code injection), the software can be changed. These attacks describe a targeted manipulation (energy supplier, user, etc.). At worst, a shutdown or manipulation of the energy grid or data manipulation and modification (energy supplier or at home) are possible. Additionally, the Cloud platforms (IoT cloud and SG cloud) can be manipulated and fail.

3) Network-based attacks: Identity theft, denial of service, cascading malware propagation (Business IT & Plant Control) and monitor, traffic analysis (passive attacks) are possible network-based attacks. At worst, personal damage to users, customers and the manipulation of the energy grid or the the cloud platforms are possible.

4) Privacy related attacks: Privacy related attacks can be, for example, collecting user-specific data (for example listening the communication). At worse, personal damage to customers or energy supplier are possible.

5) Conclusion: The analysis of the attack vectors shows us the following risks:

- manipulation of measured values and time
- manipulation of the communication between IoT cloud and SG cloud
- misuse of energy data and/or sensitive data
- sabotage of the power grid
- sabotage of mobility (example: charging station)

The IoT device, IoT infrastructure with an IoT cloud, smart meter, smart meter gateway, switching box, SG cloud and gateway administrator can be attacked in the architecture (cf. Figure 1). Summary, the security of the grid is dependent on the security of the information and communication from cloud application of IoT and SG.

B. Security threats: Infrastructure Smart Grid and Internet of Things

Table 1 covers a risk analysis for both, the IoT cloud and the SG cloud. It includes the ability of an attacker and potential damage. This leads to a risk for the associated attack. If an attacker needs a lower ability, it's more likely that someone uses the attack [10]. In the SG, the strict specifications lead to a high security and therefore the attacker must be advanced (high ability). If the attacker gets access to private data or can damage a big part of the SG, the damage is classified as high (e.g. DDoS attack on SG). For example, a medium ability and a high damage lead to a high risk [19].

The table shows that low to medium abilities are needed to attack an IoT device and its cloud. These vulnerabilities can have big impacts on the security of the SG (damage and risk). The IoT devices can be attacked easily to change the behaviour. Against wrong loading times (not much renewable energy is currently produced), the smart meter is completely exposed. It's not possible to prevent a device from loading, without limiting the comfort for the user. Other attacks, like

TABLE I. risk analysis for the IoT and SG cloud

DDoS Ability of an attacker: *low* A DDoS attack can be performed with a botnet at low cost. Damage: IoT: *medium*, SG: *high* If the SG is unable to broadcast the current amount of energy in the grid, all the connected cars start charging. In the worst case, this can lead to a shutdown of the grid. The damage is medium for the IoT because at the moment not much electric cars are available. Risk: *medium / high* The risk is medium to high because it's easy to attack and the damage is medium / high.
Malware Ability of an attacker: IoT: *low*, SG: *high* The attacker needs to find a vulnerability in the software to install a malware. In the insecure IoT, this is easily possible, because the most cheap devices never get an update. In the SG it's high because of the strict regularization. Damage: IoT: *medium*, SG: *high* The damage for the grid is medium if the IoT device is attacked (the reasons are similar to DDos). If an attacker gets access to the SG, the damage is high, because he can shutdown the critical infrastructure. Risk: IoT: *medium*, SG: *medium / high* For both IoT and SG, the risk is medium. In IoT, it's likely to happen, but the damage is similar to DDoS (medium) and in the SG, the ability of an attacker has to be high, so it's medium to high, because the damage can be high.
Broken Authentication Ability of an attacker: IoT: *low*, SG: *high* The broken authentication is similar to the malware. An IoT device is not secure at all and the SG is regulated. Damage: IoT: *medium*, SG: *high* Similar to malware. Risk: IoT: *medium*, SG: *medium / high* Similar to malware.
Broken Encryption Ability of an attacker: IoT: *low*, SG: *high* Similar to malware. Damage: *low / medium* The data, transferred to the network, is not critical for running the SG (low), but the privacy of an user can be exposed (medium). Risk: IoT: *medium*, SG: *low* Because it's easy to attack in the IoT and the privacy can be exposed, the risk is medium in the IoT. With nearly no damage, the risk is low in SG.
Data leakage The data leakage is similar to the broken encryption and therefore the same rating is used: Ability of an attacker: IoT: *low*, SG: *high* Damage: *low / medium* Risk: IoT: medium, SG: *low*
Data manipulation Ability of an attacker: IoT: *low*, SG: *high* Data manipulation can be performed easily in the IoT cloud and is difficult in the SG network (cf. broken authentication). Damage: IoT: *low*, SG: *medium* If an attacker can manipulate some data in the IoT cloud, the SG is nearly not affected. If it happens in the SG, the attack can lead to more damage, but only for a part of the user (the hacked ones). Risk: IoT: *low*, SG: *medium* This risk is low for IoT and medium for the SG.
Hardware manipulation Ability of an attacker: IoT: *medium*, SG: *high* To get on the hardware of the clouds, an attacker needs a lot ability, even in the IoT case. Damage: IoT: *medium*, SG: *high* The damage is medium in the IoT, because with the hardware attack, only one IoT manufacturer is affected. In the SG, it could lead to an shutdown of the grid. Risk: *medium* The risk is medium for the IoT and SG. The damage on the SG is high, but it's difficult to attack the SG cloud hardware.

a denial of service attack or a direct attack on the smart meter, can be detected and prevented by the right software (e.g. firewall or intrusion detection system). In conclusion, the communication between IoT devices and the smart meter should only be possible through a secure layer.

C. Communication between clouds

An IoT device and the IoT infrastructure are currently highly insecure [11]. The charging station or the IoT cloud can be hacked by an attacker (see risks above). The "SG device" is a secure device. For example, the SMGW is a certified device.

The communication between the two clouds should be transparent to the user and developed under the aspects of security and privacy by design. Both contain private data and only the user should allow an exchange. By default no data should be transferred.

Example 1: The user can register his IoT device in the IoT cloud only with a valid E-Mail address and a username. No further information is needed. The IoT provider only knows that this username has loaded his car 20 times per month. By exchanging data with the smart meter, detailed information (name, address) about the user can be transferred. Now it is possible to identify the user.

Example 2: The energy service provider doesn't need any information of the connected car of the user. But with additional information from the IoT charging station, it is possible to tell when the user is at home or if he gets visited by another person with an electric car. This part is very important. A third user can be tracked with his car, without knowing it.

The security analysis and the application example shows us problems and challenges of communication in cloud application on IoT and SG. A growing problem is the authentication and authorization. The analysis of the system shows that more and more data is being generated in the single systems, because they receive data from the other ones. This data differs in origin, need for protection, purpose, quality and volume. A further point is the constantly growing number of users who have access to the system or to the data. Users cannot only be individuals, but also devices, such as meters, sensors, etc. new risks, threats and attack patterns arise from the further development of the system. The question arises as to which requirements for authentication and authorization must be defined for future systems.

D. Requirements - authentication and authorization

The technical and organizational requirements can be derived from the application example and security analysis. The focus of the requirements is on authentication and authorisation. The security analysis shows us the weakness of communication. Future systems must be better protected against unauthorised access. The defined requirements are necessary for future development of authentication and authorization mechanism for cloud applications on SG and IoT.

The technical and organizational requirements of authentication and authorization mechanism for cloud applications on SG and IoT are defined as follows:

1) Availability: authentified and authorized users can access or use resources under defined conditions
2) Interoperability: user can be individuals and devices
3) Evidence: proof of access to the data or system to be protected
4) Performance: SG and IoT are a volatile systems
5) Scalability: SG and IoT are highly scalable systems
6) Device and user authentication: distinction should be made between device and user authentication
7) Data-Management: simple and cost-efficient management of authentication and authorisation information
8) Update-Management: ability to change information (e.g. device or device number)
9) Maintenance: simple and cost-efficient upkeep and maintenance of the system

Current authentication and authorization mechanisms are no longer sufficient for the defined requirements of authentication and authorization mechanism for cloud applications on SG and IoT. One important reason is the weakness of communication. Another reason is the increasing communication and data exchange. A new model is needed for authentication and authorization for cloud applications on SG and IoT. With this new model, the classical security model must also be reinterpreted. In the classical security model, the data is divided into two categories (secure and insecure).

V. Conclusion and future work

We introduced an application example of a connection between SG and IoT. A charging station with an own cloud, connected to the smart meter gateway. These connection creates new attack vectors and threads. For example, an attacker can use an unsecured device like the charging station to get access to the highly secured SG network. This is critical, because of the different information stored on both clouds. The energy provider stores payment information and the amount of consumed energy, the IoT cloud information about the charging times. These private information should be strongly protected and not combined.

The application example and the security analysis shows us new attack vectors and threads and challenges of communication in IoT and SG. In this paper, we focus the problem with authentication and authorization mechanism for cloud applications on SG and IoT. Current authentication and authorization mechanisms are no longer sufficient for the defined requirements. The reason for this is the increasing communication and data exchange. This leads to an increased overhead in the classical security model. The question arises as to which framework can be used for the new requirements for authentication and authorization. An option is to develop a new role-based trust model for safety-critical systems. In order to develop a more flexible model, the new approach has to integrate several data categories. To protect the data, the different information need a classification and a clear mechanism to ensure that they are only accessed by authorized users. For this task, a new Role-based trust model for Safety-critical Systems should be implemented. With this model, the occurring problems, like data exchange, can be addressed. The different data, stored by the clouds, can be classified and secured by adding an extra layer for the access. The role-based access control model ensures an efficient administration of the rights. This model is still a work in progress and the next steps will be to implement and to evaluate it.

References

[1] M. Irlbeck, Digitalisierung und Energie 4.0 Wie schaffen wir die digitale Energiewende?, Springer Fachmedien Wiesbaden GmbH, pp. 135-148, 2017.

[2] H. Kim and K. Kim, Toward an Inverse-free Lightweight Encryption Scheme for IoT, Conference on Information Security and Cryptography, 2014.

[3] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, SIT: A Lightweight Encryption Algorithm for Secure Internet of Things, CoRR abs/1704.08688, 2017.

[4] M. Uslar, C. Rosinger, and S. Schlegel, Application of the NISTIR 7628 for Information Security in the Smart Grid Architecture Model (SGAM), VDE Kongress, 2014.

[5] Bundesamt fuer Sicherheit in der Informationstechnik, Technische Richtlinie, BSI TR-03109, 2015.

[6] P. Peters and N. Mohr, Digitalisierung im Energiemarkt: Neue Chancen, neue Herausforderungen, Energiewirtschaftliche Tagesfragen, pp. 8-12, 2015.

[7] C. Eckert, IT-Sicherheit, Konzepte - Verfahren - Protokolle, Boston De Gruyter, 2012.

[8] R. Sichler, Smart und sicher geht das?, Springer Fachmedien Wiesbaden, pp. 463-494, 2014.

[9] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, Proposed embedded security framework for Internet of Things (IoT), Electronic Systems Technology (Wireless VITAE), 2010.

[10] L. ben Othmane, H. Weffers, and M. Klabbers, Using Attacker Capabilities and Motivations in Estimating Security Risk, Symposium On Usable Privacy and Security, 2013.

[11] The OWASP Foundation, Internet of Things Project, IoT Vulnerabilities, 2019.

[12] M. Lipp, et al., Meltdown: Reading Kernel Memory from User Space, 27th USENIX Security Symposium, 2018.

[13] P. Kocher, et al., Spectre Attacks: Exploiting Speculative Execution, CoRR abs-1801-01203, 2019.

[14] F. Dalipi and S. Y. Yayilgan, Security and Privacy Considerations for IoT Application on Smart Grids. Survey and Research Challenges, IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pp. 63-68, 2016.

[15] M. Yun and B. Yuxin, Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid, International Conference on Advances in Energy Engineering, pp. 69-72, 2010.

[16] V. C. Gungor, et al., A Survey on Smart Grid Potential Applications and Communication Requirements, IEEE Trans. Ind. Inf. 9 (1), pp. 28-42, 2013.

[17] X. Li, et al., Securing smart grid. Cyber attacks, countermeasures, and challenges, IEEE Commun. Mag. 50 (8), pp. 38-45, 2012.

[18] C. Wietfeld, C. Muller, J. Schmutzler, S. Fries, and A. Heidenreich, ICT Reference Architecture Design Based on Requirements for Future Energy Marketplaces, 1st IEEE International Conference on Smart Grid Communications, pp. 315-320, 2010.

[19] The OWASP Foundation, OWASP Risk Rating Methodology, 2019.

[20] B. Genge, A. Beres, and P. Haller, A survey on cloud-based software platforms to implement secure smart grids, 49th International Universities Power Engineering Conference (UPEC),pp. 1-6, 2014.

[21] S. Bera, S. Misra, and J. Rodrigues, J.P.C: Cloud Computing Applications for Smart Grid. A Survey, IEEE Trans. Parallel Distrib. Syst. 26 (5), pp. 1477-1494, 2015.

[22] Y. Simmhan, A. G. Kumbhare, B. Cao, and V. Prasanna, An Analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds, IEEE 4th USENIX International Conference on Cloud Computing (CLOUD), pp. 582-589, 2011.