INFORMATION
SYSTEMS IN
MANAGEMENT

Information Systems in Management (2013) Vol. 2 (3) 239–249

SMART METERING AND DATA PRIVACY ISSUES

TOMASZ ZĄBKOWSKI, KRZYSZTOF GAJOWNICZEK

Faculty of Applied Informatics and Mathematics
Warsaw University of Life Sciences – SGGW

Growing energy consumption enforces initiatives that look for alternatives aimed at better energy management and load balancing. Smart metering is a topic that meets these expectations and it seems to provide a value added for both, suppliers and customers. In this paper we focus on different issues of data and privacy protection for smart grids. In particular, we discuss security concerns related to system architecture, possible means of data protection and demonstrate the main research challenges in privacy assurance for smart grids.

Keywords: smart metering, data protection, privacy protection

1. Introduction

In general, smart metering concerns the usage of some intelligent metering devices at customer location and the regular process of reading, processing and giving the information about consumption to the customer. It needs to be stated that there is a clear distinction between a smart meter and smart metering. The first one is the individual device installed at customer house or facility, primarily measuring the energy consumption. The second one, is a general application of smart meters on a larger scale, connected in a grid. In particular, EU legal framework refers to "intelligent metering systems". The European Commission's Interpretative Note on Directive 2009/72/EC [8] gives a description of the Commission's understanding of a metering system which is *"the ability to provide bi-directional communication*

between the consumer and the supplier/operator and to promote services that facilitate energy efficiency within the home."

Smart metering appears to be a remedy for rising prices of electricity and therefore, to encourage parties involved there are many benefits attributed to smart metering systems.

From the individual customer point of view (end user) the main benefits include [6, 7]:

- Access to detailed data to manage energy usage;
- More accurate and timely delivered billing;
- Possibility to benefit from demand flexibility;
- Possibility to introduce safety solutions of the household and equipment through better power quality and breakdown management;
- Other, such as home appliances failure detection, detection of waste, detection of unexpected activity or inactivity, what could be possible with smart home unit controllers.

For the energy supplier, the smart metering offers, among others [6, 7]:

- Possibility to introduce demand response approach what is especially important on electricity market dealing with peak loads;
- Reduced costs of metering readings compared to manual data gathering;
- Reduced back office rebilling process;
- Misuse and fraud detection;

On the other hand there are also costs associated with smart metering implementation. It is clear that the implementation of smart meters will entail number of costs, including the initial cost of the meters, communications costs and also possibly higher maintenance costs of electric devices.

Nevertheless, a serious costs related to smart metering systems concern customer data protection and privacy assurance. Therefore, while building the smart metering infrastructure and dedicated solutions a special attention should be paid to data protection and security issues in order to ensure secure data communication and protection of consumers private data against unauthorized access or hacking.

The purpose of the article is to systematize different issues of data and privacy protection for smart grids. In particular, we discuss different security concerns related to system architecture, possible means of data protection and demonstrate the main research challenges in privacy assurance for smart metering solutions.

2. Smart metering architecture and data flow

ICT (Information and Communication Technologies) systems including smart metering and grid automation possesses functionality, security and real-time

requirements that need to be fulfilled as whole and in a way that is technically and economically feasible. Security threats in smart meter solutions include data tampering in order to manipulate the billing, leakage of private data related to the lifestyle and financial situation of customers, and finally manipulation of grid control commands, which can threaten the whole network.

Particular challenges arise due the large scale of a smart grid and because system components are widely distributed in the field. For this reason the components need to be very stable and secure, particularly in the light of cyber security concept. This concept is defined to be aware of threads conveyed by computers and the protection of the assets from modification or damage from accidental or malicious misuse.

A typical smart metering architecture consists of the following elements [2]:

1) Metering device with associated devices on the customer's site, which can be optionally connected to a smart home controller to manage appliances usage (taking into account tariff information and energy costs);
2) Communication and data processing infrastructure between the customers devices and the transactional systems of the utility supplier;
3) Central data management system which is located on supplier's site and it has possibility, inter alia, to start/shut down the utility supply, to process data for customer relationship purposes, to archive data according to legal requirements and and optionally to present data to the consumers, through the web page, for instance.

This system is formed by a collection of software, hardware, operators and information flow. However, for the sake of consistency, we will now briefly describe the parties involved in a smart metering showing that they are cross related not only due to electricity flow but also data flow. As shown on Fig. 1 we can distinguish:

- Customers (individual and business); They are end-users that receive the power supply. They generate usage patterns and specific individual consumption information. These are sensitive data that must be protected for preserving the consumers' privacy. It is assumed that customers would have access to the data on various granularity levels in order to select an advantageous tariff and be able to manage their usage habits and electric appliances.
- Smart metering devices; They are installed at the customer location in order to record the consumed energy at different time windows and send the measurements to the customer and/or the aggregator. Each customer must be equipped with at least one meter, so they are typically small and cheap devices with limited computational power.
- Grid operator (Supplier); This is a company that controls the electricity distribution and transportation infrastructure. Data flow for the operators is

crucial since they may employ electricity usage data and distribution needs in order to manage their resources. With detailed consumption data a better load balancing is feasible.

– Communication network; It concerns communication among all the parties involved in the smart meter grid. Due to sensitive data transmission all communication channels must be secured.
– Electricity producer (power plant); This is a company that produces and then sells the electricity to the customers through the supplier's infrastructure. The producer must take into account demand data (to adjust the produced electricity), and total consumption data for billing each consumer according the contracted tariff.

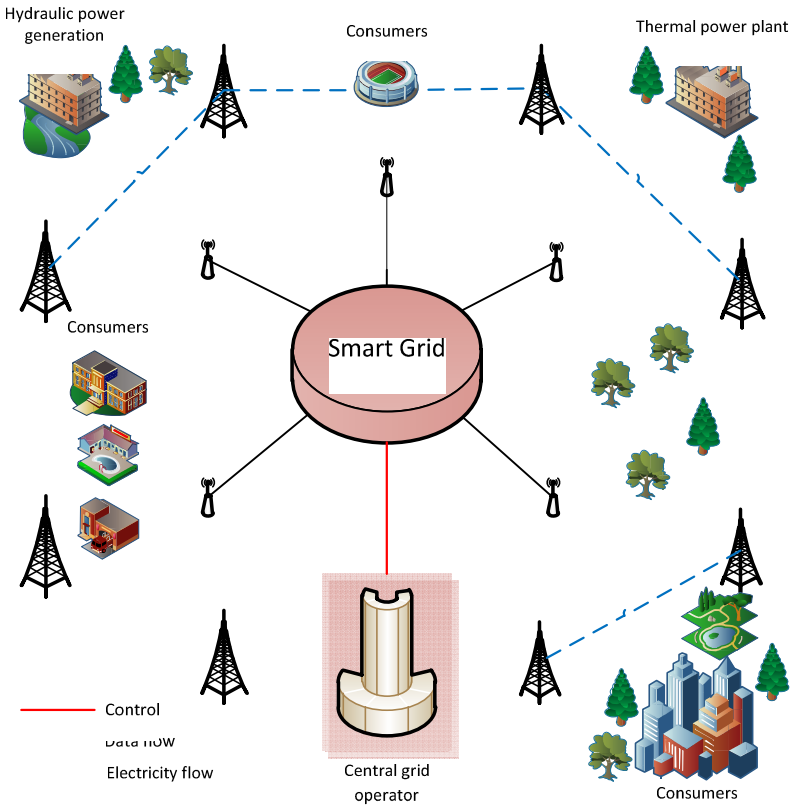

Figure 1. Scheme of example smart meter architecture

A fully centralized architecture gives the meters only the sensing function, with ability of sending the measurements to a central database. The database acts acts as a node and communicates with each smart meter. The data stored in

database is then used for consumption calculation, load balancing and billing. Each customer may access the stored data in order to get information about own consumptions. This approach seems to be considered as dominating scenario for smart metering implementation proposals.

A centralized management and data collection implies a trust on the grid operator as this party who would play the role of the chief data officer concentrating also the authentication and storage functionalities, and having access to all the fine-grained measurements, stored in a central database.

Undoubtedly, it possesses many technical and legal difficulties for the delivery of an actual and appropriate privacy preserving solutions.

3. Smart meter data and privacy concerns

There are two European directives that are relevant to data processing in smart meters:

1. The European Data Protection Directive which governs the processing of personal data by data controllers and grants rights to individuals.
2. The European Privacy and Electronic Communications Directive which aim to make it technology neutral.

Under these directives a number of requirements concerning data protection is specified. Firstly, personal data processing is allowed only if specific legal purposes apply. Secondly, personal data gathered for one purpose cannot be used for another purpose without permission. Thirdly, there are limitations on the personal data transfer to other countries. Finally, there is a strict obligation to ensure adequate security.

For this reasons, smart meters cannot transmit any sensitive data such as customer name or address, but to some extend it will involve transmitting personal data through the use of a smart meter ID number, which can be associated with a recipient. The information that smart meters will transfer from the customer to the supplier would include:

- smart meter ID number;
- meter readings on different granularity level;
- type of information transmitted (meter reading or unauthorised access alert);
- date and time;
- payment details for the customers using prepayment meter.

Readings from the smart meter will be gathered through remote access to prepare energy usage profile of the individual or the household. Supplier will be able to use those behavioural data (for instance, low energy usage when the customer is away from home) to prepare kind of energy profile. This can be basis for new services and new tariffs developments based on such energy profiles.

For this reasons, data collected from smart meters will be interesting both, for energy suppliers and consumers.

As the smart meter technologies will capture personal data, energy suppliers will be data controllers and responsible for acting with data protection laws, even if they outsource any data processing services. In fact, energy suppliers already have to comply with data protection laws, so the main requirement concerning existing obligations is adequate enforcement. If final arrangements concerning smart meter solutions take the form of supplier centric approach then data capture, use, storage and sharing will be domain of the energy supplier. Then a question arises: what would energy suppliers do with the data they get from customers? Although there are customers who are in favour of smart meters as a way of providing them more accurate and detailed usage information, some people are concerned about how suppliers will use the energy consumption data arguing this would be an invasion of privacy.

Therefore, there is a need for providing clear and understandable for the customers rules on:

- data capture including the clear statement of what data are allowed to be captured, stored in databases and for what purposes;
- data use (how the customer data are used);
- data storage (how the data are stored ad if they are secured);
- data sharing (what data and how can data be shared with other parties).

Some parties (customers lobby and governments) indicate a need for wide consultation [3] to tackle some key questions such as:

- Should the regulations limit data capture to only that which is necessary for the maintenance and proper functioning of the service?
- Should the regulations limit data usage in any way?
- Should the regulations provide limitations on data storage?
- Should the regulations provide further guidance on data sharing?

Some societies and movements which are opposed to the introduction of smart metering initiatives in United States compares it to the Big Brother's and argue that it is against The Fourth Amendment (Amendment IV). It is the amendment to the US Constitution which is the part of the Bill of Rights that prohibits unreasonable searches and seizures and requires any warrant to be judicially sanctioned and supported by probable cause.

We have underlined that privacy is a crucial issue in smart metering. With a short example we can show possible privacy violation produced when collecting fine-grained readings from a household power consumption. These are real data gathered for the purpose of smart metering project in one of the households in Warsaw in September and October 2012. Such data reveals information about in-home activities that can be mined and combined with other available information to discover more about inhabitants' behaviour.

Fig. 2 represents a set of hourly readings for a time span of 400 hours, where the non-consumption period of the household can be easily identified just by eye inspection. This so called "inactivity" period falls on a weekend and this information is very sensitive since it shows theoretical risk concerned with detailed data collection, as it could be used to find out when a home was empty in order to commit burglary, for instance.

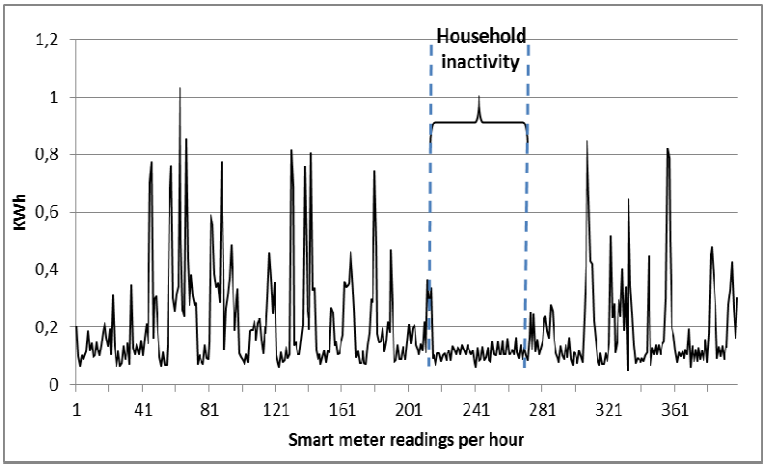

Figure 2. Household's hourly smart meter readings

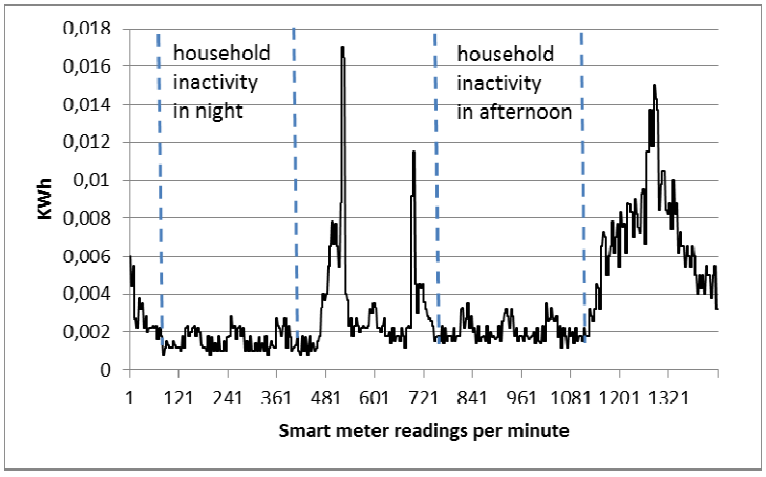

Figure 3. Household's smart meter readings per minute

Similar case is shown on Fig. 3, in which a set of minute readings for a time span of 24 hours is presented. There, we can distinguish two periods of household

inactivity. One is due to the rest during the night hours and the second one is evident during the afternoon hours. This example reflects of how important privacy protection will be when smart metering is widely deployed.

4. Challenges in data protection assurance

In this part we aim to identify and present several important challenges for considering the privacy issues in smart metering systems, taking into account their importance and influence on ease of adoption.

4.1. Challenges concerning the trust among the parties involved

Taking into account any privacy related scenario, there is an inherent dependency between the trust and privacy. According to [5] *"(...) every entities, parties and infrastructure elements of a smart metering network that are trusted will need no privacy protection, and those elements in which privacy is enforced through a secure protocol will not need to be trusted"*. Therefore, the definition of the trust model is extremely important for proper and effective customers privacy assurance. In case of smart metering scenario, the main trust relationships are established between the customers, the suppliers and grid operator. Customers' trust is directly related with privacy of the metered data and it should be stated clearly which parties can access these data for a legitimate purpose. Conversely, the trust from the supplier or grid operator is focused on the data correctness, to provide the actual usage values without trying to forge these measurements and the corresponding bills. The traditional sealed meters accessible only at the customer's location represented the mutual trust between the supplier and the customers, in a way that customers could not forge the measurements without manipulating the meter and the operator could only access approximate measurements. Therefore, adoption of smart metering changes the trust model and evolving it towards relation that is based on mutual trust, also taking into account the choice of system architecture.

4.2. Challenges concerning the smart meter hardware

For the smart metering growth to be economically feasible, from the grid operators point of view, smart meters devices must be cheap and easily replaceable. This corresponds to a scalability, what means that cost of meter devices deployment at users' locations must be manageable and must be covered by the energy savings and consumption reduction as a result of smart use and the optimal load balancing. Therefore, smart meters cannot be well equipped and high performance computers but rather small devices with very limited computation resources and importantly characterized by small power consumption.

Due to these fundamental limitations, some of the proposals for privacy-preserving have addressed the use of simple homomorphic encryptions which is the conversion of data into cipher text that can be used or read as if it was still in its original form. Existing current meters don't possess trusted elements capable of performing complex homomorphic encryption. Even if they have, they use symmetric cryptography [10] usually supporting rather light cryptographic functions like hashes and secret-key encryption/decryption and hash-based message authentication code signatures. Most of the proposed privacy preserving solutions require [9] application of tamper-proof cryptographic modules (similar to smart cards) to handle integrity, distributed authentication and heavy public key data encryption and signatures. Accordingly, if homomorphic processing is chosen then the smart meter devices must also cope with homomorphic operations that include large modular additions, multiplications and exponentiations [9]. This may be too difficult to achieve assuming the low manufacturing cost of these devices.

4.3. Challenges related to cryptographic protocols

In case of the system in which the grid operator company has the control and concentrates the need of trust from the customers, customers will assume that they will be billed correctly for their consumptions. On the other hand, if customer privacy is respected and guaranteed, then it is the utility company who must trust that the measurement and billing calculation are correctly performed, as it will not have access to particular individual measurements. That is why the grid operators are very sceptical to adopt a privacy preserving solution if it does not appear next to fraud detection mechanism and technical guarantees that cheating customers will not take place.

For private protocols based on homomorphic encryption [4], *"(...) it is a common requirement that all the encrypted values are produced with the same key in order to be homomorphically combinable in such a way that the secret key is shared among several customers and even the utility company"*. In a typical setting, key disclosure would imply losing the possibility of correct authentication. The other problems would include the risk of forgery by users familiar with the technology and decryption techniques. The solution to these problem is, for instance, unusual key distribution mechanisms, like the sub-key generation process proposed by [4] or the peer-to-peer key establishment by [1]. The last one concerns the case, in which each two coupled users share a uniquely computed key for each iteration of the private consumption calculation protocol.

Surely, for privacy protection, the on-going research should also invest in cryptography, also getting familiar with its benefits and certain limitations and, as a result to work out a good solution that is feasible to adopt in smart metering infrastructure.

5. Conclusions

In this paper, we identified a set of data protection and privacy problems in smart grid architecture and present an overview of existing research challenges for secure data processing what brings us towards better understanding of both, customer and system operator needs.

The mainstream of the smart metering systems critique is that it collects personal information. Customer data are collected and it gives a possibility for utility providers to monitor customers behaviours. In order to assure a customer privacy and data protection a certain initiatives should be undertaken, including (1) guidelines regulating access to data for customer service, (2) strong user control over information leaving the customer location, (3) protocols that can process most of the data at customer locations.

Undoubtedly, the topic is very complex and difficult since it tackles very sensitive issues. However, the consensus appears to be possible to achieve assuming that each of the parties involved would show a good will.

Acknowledgments

This research was financed by VEDIA S.A. leading a project partially supported by National Centre for Research and Development (NCBiR).

REFERENCES

[1] Acs G., Castelluccia C. (2011) *I have a DREAM! (Differentially PrivatE smart Metering)*, Information Hiding Conference, May 18-20 2011. http://www.crysys.hu/~acs/publications/AcsC11ih.pdf [access on 03/10/2013]

[2] Bator M., Orłowski A., *Ząbkowski* T. (2012) *Smart Metering – a brief overview of projects, benefits and applications*, Information Systems in Management 1(1), 72-83.

[3] *Department* of Energy and Climate Change (2012) *Smart Metering Implementation Programme, Data access and privacy, Government response to consultation*, London http://www.decc.gov.uk/en/content/cms/consultations/cons_smip/cons_smip.aspx [access on 02/10/2013]

[4] Erkin Z., Tsudik G. (2012) *Private computation of spatial and temporal power consumption with smart meters*, International Conference on Applied Cryptography and Network Security June 26-29, 2012, Springer-Verlag, 561–577.

[5] Erkin Z., Troncoso-Pastoriza J., Lagendijk R., Perez-Gonzalez F. (2013) *Privacy-preserving data* aggregation *in smart metering systems: An overview*, Signal Processing Magazine, IEEE, 30(2), 75–86.

[6] European Smart Metering Alliance [ESMA] (2008*) Definition of Smart Metering and Application and Identification of Benefits*

http://www.vtt.fi/inf/julkaisut/muut/2008/Definition_of_smart_metering_and_applications_and_identification_of_benefits.pdf [access on 30/09/2013]

[7] European Smart Metering Alliance [ESMA] (2010) *Smart Metering Guide Energy Saving and the Customer*, http://www.ecn.nl/docs/library/report/2011/o11004.pdf [access on 30/09/2013]

[8] EU Commission Staff Working Paper (2009) *Interpretative Note on Directive 2009/72/EC Concerning Common Rules for the Internal Market in Electricity and Directive*, Brussels, 22 January 2010. http://ec.europa.eu/energy/gas_electricity/interpretative_notes/doc/implementation_notes/2010_01_21_the_unbundling_regime.pdf [access on 30/09/2013]

[9] Garcia F.D., Jacobs B. (2010) *Privacy-friendly energy-metering via homomorphic encryption*, 6th Workshop on Security and Trust Management (STM 2010), Lecture Notes in Computer Science, 6710, 226–238.

[10] Keemink S., Roos B. (2008) *Security analysis of dutch smart metering systems. Technical report*, Universitait van Amsterdam, July 2008. http://staff.science.uva.nl/~delaat/rp/2007-2008/p33/report.pdf [access on 05/10/2013]