Security in Large-Scale Data Management and Distributed Data Acquisition

Alexander Kramer, Wilfried Jakob, Heiko Maaß and Wolfgang Süß
Institute for Applied Computer Science, CN, Karlsruhe Institute of Technology (KIT), P.O. Box 3640, 76021 Karlsruhe, Germany

Keywords: Security, Privacy, Scalable Data Exchange, Smart Grid Data Management, Generic Data Management.

Abstract: The internet is about to change from a pure network of computers to a network of more or less intelligent devices, the computer being just one of them. Examples of this change are the concepts of smart applications like smart homes, smart traffic control and guidance systems, smart power grids, or smart buildings. These systems require among others a high degree of robustness, reliability, scalability, safety, and security. In this paper, we concentrate on the data exchange and management aspect and introduce a security concept for scalable and easy-to-use Generic Data Services, called SeGDS. It covers application scenarios from embedded field devices for data acquisition to large-scale generic data applications and data management. The concept is based largely on proven standard enterprise hardware and standard solutions. As a first application, we report about transport and management of mass data originating from high-resolution electrical data devices, which measure parameters of the electrical grid with a high sample rate. The shown solution is intended to be a contribution to concepts of a secure, flexible, but comparably inexpensive management of large amounts of data coming from modern smart power grids or other comparable smart applications.

1 INTRODUCTION

Examples of new smart application concepts demanding high rates of data exchange are smart traffic control and guidance systems, smart buildings, or smart power grids. As the latter shows a number of issues typical of such systems, we take a closer look at it. The old electrical supply system, which served mainly as a centralized power distribution network, is currently changing to a much more decentralized grid with a growing number of volatile energy sources. In addition, it is intended that the power consumption of more and more grid nodes can be influenced to some extent by a net supervisory system aiming at an increasing steadiness of the network load (German Fed. Min. of Economy and Energy, 2012; U.S. Dept. of Energy, 2014). Controlling the stability of such a power system is a much more complex task than the control of the old one and requires data acquisition in real time (Bakken *et al.,* 2011). As a result, we have three types of data: Data on the consumption and feeding for billing purposes, data for consumption control, and data about the network status to control the stability of the network itself. All these data have in common that their confidentiality must be ensured. Data for billing and consumption control require privacy by nature and data about the network status must also be protected as they can be used for an attack on the network as well as for ensuring its stability (ENISA, 12.7.2012). Smart meters usually provide 1-15 minute values consisting of cumulated power values over time. In contrast to that, data for network control are required in real time, which means at the level of a few seconds or less (Bakken *et al.,* 2011). Both applications produce a large amount of data to be securely transferred, either because there is a large amount of data sources as in case of smart meters or because the update frequency is high.

Another important aspect is the dynamic nature of security and reliability. Both interact and the threats change over time. The more dissemination and diversity of any smart application increase, the larger does the vulnerability of the entire system grow. New threats will occur, which cannot be foreseen today. Thus, security measures are not a one-time business, but a permanent process

Kramer A., Jakob W., Maaß H. and Süß W..
Security in Large-Scale Data Management and Distributed Data Acquisition.
DOI: 10.5220/0005095901250132
In *Proceedings of 3rd International Conference on Data Management Technologies and Applications* (DATA-2014), pages 125-132
ISBN: 978-989-758-035-2

throughout the entire life cycle of a network and of all of its components.

These considerations lead to the following requirements:

a) Scalability:
   New networks like smart power grids will start with a comparably small number of metering devices, but their number and data rates will grow over time.
b) Heterogeneity:
   Devices and software tools of different vendors used for different purposes and producing various data rates must be integrated.
c) Suitability for different IT infrastructures
d) High reliability:
   Online network control, for instance, requires an availability of close to 100%.
e) High degree of safety:
   Many people will only accept smart grids as long as their privacy is secured. Data integrity must be ensured as well. The reliability of the power supply net is all the more essential the more a country is industrialized.
f) Maintainability:
   New security threats may require a fast reaction and, thus, it must be possible to quickly upload software updates to the affected components of the network. Furthermore, it must be possible to replace outdated security, transmission, or other methods and standards by up-to-date ones.
g) Cost effectiveness:
   The smart power grid is to be a mass product. Acceptance of consumers requires low costs of the devices and services.
h) Restricted access and logging:
   Access must be restricted to authorized personnel. Logging of all transactions is required to allow for a detection of attacks and misuse.

To handle diverse data and to facilitate different kinds of data processing, a flexible data management system is required. For this purpose, we developed our metadata-driven concept of Generic Data Services (GDS), see (Maaß *et al.,* 2012; Stucky *et al.,* 2014), a first prototype of which was implemented for handling voltage measurement data of a very high resolution (12.8 kHz) needed for ongoing research projects (Maaß *et al.,* 2014; Bach *et al.,* 2012). These devices are called Electrical Data Recorders (EDR). Furthermore, the GDS stores the electric circuit plan of the Campus North of KIT, which is a classified document due to the shut down and operating nuclear installations, which have to be protected against terrorist attacks. The plan is required for the development of sub-models of the network, which serve as a basis for simulations and studies. Thus, GDS must provide a high degree of safety, especially as it is operated in an environment with a large number of users: More than 24,500 students and about 9,400 employees have access to the KIT LAN. This implies that administration of the comparably small number of GDS users must be separated completely from the user management of KIT.

In this paper we will introduce a concept for secure and reliable data transport, storage, and management, which will meet the above demands. It is based on standard hard- and software solutions and standardized interfaces, which considerably facilitates the fulfillment of a part of the listed requirements. In particular, the reliance on standardized interfaces follows directly from the heterogeneity and maintainability requirements. The rest of the paper is organized as follows. Section 2 gives a brief overview of related work. Our security concept is introduced in section 3 and compared with the previously established requirements, while section 4 reports about the first prototypic implementation. The last section summarizes the paper and gives an outlook on future work.

2 RELATED WORK

IT security is a topic which is about as old as IT itself. Risks and threats grew with the growing capabilities of IT systems to today's cyber threats and challenges, see e.g. (Menezes *et al.,* 1997; Ferguson *et al.,* 2010; Partida and Andina, 2010; Yu and Jajodia, 2007). To secure data communication via the internet, several attempts have been made resulting in standards like IPSec (Doraswamy and Harkins, 2003; Stallings, 2013), TLS/SSL (Rescorla, 2000; Oppliger, 2009), or the concept of virtual private networks (VPN) (Doraswamy and Harkins, 2003) based on these secure communication standards.

Berger and Iniewski give an up-to-date overview of smart power grid applications and their technologies, including different communication techniques, and provide an in-depth discussion on the related security challenges (Berger and Iniewski, 2012). Mylnek et. al. propose a secure communication based on a selected encryption method, but it is intended to support only low-cost and low-power grid devices and thus, the concept

lacks flexibility with respect to future requirements (Mlynek *et al.,* 2013). Also IT infrastructure suppliers like Cisco (Cisco Systems, 2011), Juniper (Juniper Networks, 2014), or IBM in conjunction with Juniper (IBM Corporation, 2014) develop concepts for smart grid security and grid networking. A completely different approach is pursued in (Li *et al.,* 2011), where an incremental data aggregation method for a set of smart meters is proposed to protect user privacy. For further and permanently updated information, see the IEEE web portal on smart grids (IEEE, 2014), where also security aspects are discussed.

A very good overview of the current state of the art about IT security is given in (Eckert, 2012).

3 SeGDS CONCEPT

Before the security concept is described, we briefly introduce the GDS. Is is an object- and service-oriented data management system designed to manage large amounts of data stored e.g. in the Large Scale Data Facility (LSDF) of KIT (García *et al.,* 2011). It is generic in so far, as it can deal with differently structured data and different kinds of storage systems. For this purpose, three kinds of metadata were defined: Structural metadata describe the structure of the data objects to be handled, while application metadata (AMD) are used to identify a data object. Thus, the AMD must be unique. It is left to the user to define which data shall serve for this identification purposes. It can be either a set of different user data or an identifier which is provided and managed by the application. The only requirement is its uniqueness. The third class of metadata is called organizational metadata (OMD) and it is used to manage the localization of data objects in storage systems and to handle security issues as described later in this section. Data objects are stored always as a whole and AMD are stored additionally as a metadata catalog. For the latter, the GDS uses its own data-base system, which is separated from the mass storage system used. A detailed description of the GDS in general and its metadata-based concept can be found in (Stucky *et al.,* 2014).

The concept of the Secure GDS (SeGDS) comprises:

- Secure data transport between clients and the GDS services, including authentication as described in sections 3.1 and 3.2.
- The aggregation of objects to be treated equally with respect to safety, see section 3.3.
- Ciphering and pseudonymization discussed in section 3.4.
- The management of users, user groups and access rights, see section 3.5.

3.1 Overall Concept

The requirements *a, b, d, f*, and *g* from the above list suggest a solution based on standards rather than application-specific approaches. Cost effectiveness (g) of a scalable (a), heterogeneous (b), and highly reliable IT system, which can be updated quickly and adapted easily to new upcoming methods (f) requires standards. To achieve a high level of safety (i), communication must be isolated and encrypted. At least in the beginning, the existing communication infrastructure has to be used to achieve low costs. Thus, we decided to use a virtual private network (VPN) based on standard hardware solutions to connect data acquisition devices like smart meters or more highly sophisticated devices like EDRs and user applications to the GDS via the present and insecure internet. This ensures scalability to a large extent, as the internet concept proved that it is highly expandable in the last 20 years. This also applies in the case of the establishment of a separate network from the internet, which may become necessary to avoid disturbances by load peaks of the public part of the network. As TLS/SSL has turned out to be mostly used for cyphering by clients, we recommend this secure communication method as well. The VPN shifts the burden of authentication from the application, here the GDS, to the VPN itself, as only registered users, who can authenticate themselves, are granted access (h). The practice shows that VPNs fit very well into different IT infrastructures and as they are independent of the structure of the data transferred, requirements *c* and *e* are also met. The growing amount of data (a) remains a critical point, especially since the data must be encrypted and decrypted. On the other hand, cyphering is a fundamental requirement regardless of the use of a VPN. As with the internet before, growing data volumes will require faster and/or more parallel hardware and communication lines.

Figure 1 shows the overall concept. The clients are connected to the *VPN router* farm via the internet. The VPN routers share the traffic (load balancing) and pass it on to the alternatively usable *GDS Servers* and operate in failover mode, so that the service of a defective device can be taken over by others with the performance being reduced to some extent only. Authorization is done here by a

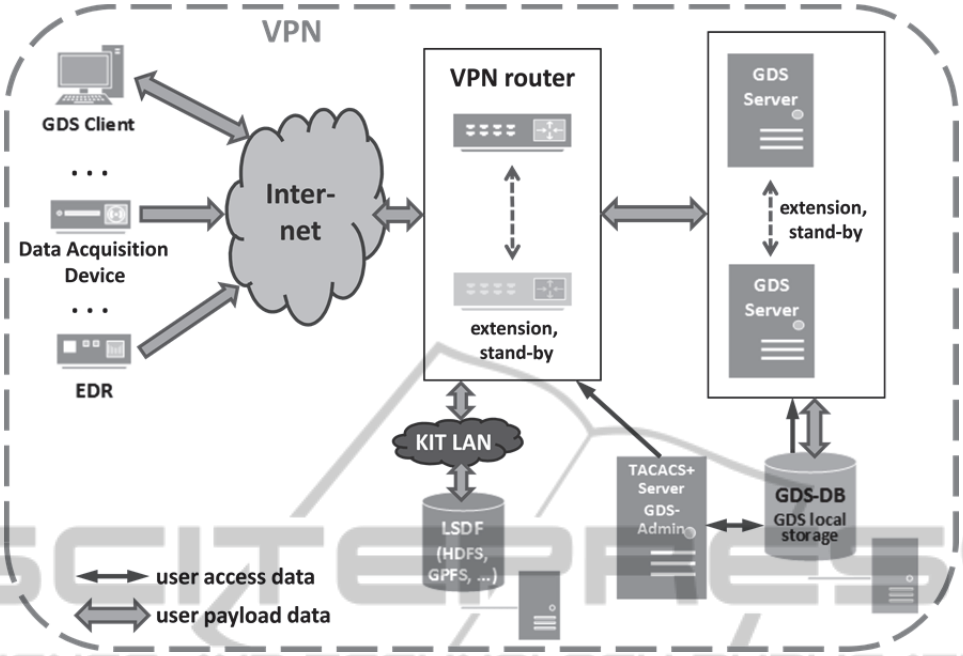

Figure 1: Overall concept of the SeGDS virtual private network.

TACACS^{+}*-Server*, which reads the user information, consisting among others of the user names and encrypted passwords, from an XML configuration file. The file is generated by the *GDS-Admin* component after a change of the user list in the GDS data-base (*GDS-DB*). This results in a complete separation of the user management of VPN and GDS from the domain in which the SeGDS equipment is running. And it ensures that both components, the VPN and the GDS, work with the same user list. After successful authentication, different users are given different possibilities of access to the services of GDS according to the specifications of the access control lists. Data acquisition devices, for instance, will have access to appropriate services only, while human users or their applications may be granted extended or full access.

The *GDS-DB* shown in Figure 1 is also used to store the already mentioned AMD and OMD of the data objects. The latter will be discussed in more detail in section 3.5.

3.2 Secure Data Transport and Storage

The security of the data transported between the clients and the GDS is ensured by the encryption methods used by the VPN. The GDS decides according to given rules (Stucky *et al.,* 2014) where the data objects are stored. At present, either one of the file systems of the LSDF like the operating HDFS or the planned GPFS is used or the data are stored by the *GDS local storage* system. The latter also serves for experimental setups such as performance measurements, comparisons of different cyphers, or the like. According to the concept, the LSDF storage systems should be accessed via the VPN to ensure a maximum of safety. But this must be left to a future enhancement, as will be described in section 4.

Stored data must be protected against loss and change. The first threat is covered by the standard backup procedures of the computer center hosting the LSDF or the local storage of the GDS. Alterations of data can be detected by cryptographic hash values resulting from algorithms like SHA-2 or the upcoming SHA-3 (NIST, 2014), which are computed and saved when the data are stored. When reading the data, its integrity is checked by calculating the hash value again and comparing it with the stored one. In case of corrupted data, the standard data backups of the data center, in our case the LSDF, can be used to restore the original version.

3.3 Data Objects and Object Sets

It is assumed that many elementary *data objects* can be treated equally in terms of access rights and encryption. These objects form an *object set*. For the sake of generality, object sets may also have only

one or a few objects, but this is not expected to be the ordinary case. Every elementary data object belongs to exactly one object set.

3.4 Pseudonymization and Ciphering

In many cases, a pseudonymization of personal data may be considered a sufficient measure to provide privacy and to allow e.g. processing for statistical purposes. It is assumed, of course, that the pseudonymized data cannot be reconstructed, which is an application-dependent question.

If pseudonymization is not sufficient to protect privacy and/or if it is required by the user, all data objects of a set may be stored encrypted to provide security against unauthorized and illegal access to an external mass storage system like the present HDFS of the LSDF. There is a key per set, which is administrated by the GDS. The GDS performs encryption and decryption, so that the ciphering is completely transparent to the user except that access may slow down.

An additional security level can be provided, if the user application does the ciphering and the data objects arrive at the GDS already encrypted. In this case, the GDS needs the identifying metadata in cleartext only.

Anonymization is another issue that will be dealt with. Since the current applications do not allow anonymity, but only pseudonyms, anonymization is processed later.

3.5 Users, Groups, and Access Rights

As with many other data administration systems, we have *users*, who may be merged into *groups*, provided that they have the same *access rights* to object sets.

3.5.1 Users and their Properties

Every registered application or person is a *user*, who may be a member of one or more groups. It is distinguished between ordinary users and *administrators*, who have special rights, as will be explained later.

Each object set is owned by exactly one user. Users may, but need not possess one or more object sets.

Every user has a default object set, to which new data objects belong, provided that the writing GDS service is not told to use a different one. The default object set may, but needs not be possessed by the user it is associated with. This means that it is possible that a user stores data objects belonging to an object set, which is not his own. The idea behind this is that it may be meaningful for some automatic data sources to store their objects into the same set, which belongs e.g. to the operator controlling these sources. For reasons of security, every device acts as a separate so called device-user, which can log-in at the same time only once. Thus, a further attempt to login can be detected easily. This does not limit the scalability, as new device users can be cloned quickly from a predefined standard schema.

Users may be permanent or temporary. This is also motivated by the automated data sources like the EDRs or other data acquisition devices, which may send data for a limited duration only. This possibility of time-limited validity of users may also be used to grant access to persons for a limited period of time, for example to students doing an internship. As users may possess object sets and object sets must be owned by someone, a user may not be deleted automatically upon deactivation. Thus, the system must not only distinguish between permanent and temporary users, but also among temporary users who are active, passive and waiting for their activation, or passive due to time-out. Temporary, expired users remain in the system until they are erased by an administrator as described in section 3.5.4.

3.5.2 User Groups

A *group* consists of users with the same access rights to some object sets in each case. A group consists of one user at the minimum and has access to at least one object set. Object sets can be accessed by no, one, or more groups. As an object set must always be possessed by a user, there is still access to a set, even in the case of no group being left with permissions to access it.

3.5.3 Access Rights

There are three basic access rights:

- Read permission
  In addition to reading all data objects of an object set, the creation of lists according to different criteria (search lists) is allowed.
- Write permission
  Allows creating a new data object
- Delete permission
  Permission to delete single data objects or an entire object set, including its data objects.

For updates of already existing objects, both rights the read and the delete permissions are

needed. These three access rights determine the access capabilities of a user regarding his own data sets or of a group concerning any data sets. Regarding his own data sets, a user can change the access rights of himself as the owner or of a group.

In addition to these user-changeable access rights to data sets, every user has a set of so-called *static rights*, which can be controlled by administrators only. They consist of the same access rights as before and can generally switch on or off a particular access right of a user. The rationale for that is to have a simple possibility for administrators to reliably limit the rights of a user without the need to consider his group rights and without allowing him to modify that even in case of his own object sets.

3.5.4 Management of Users, Groups, and Object Sets

Administrators are users with special additional capabilities. Only administrators can manage users and groups. They can give themselves all access rights to object sets and they can change the ownership of object sets as well as the access rights of the new owner. This ensures maintainability of the GDS even in case of permanent absence of a user: All the data sets of such a user can be modified so that the data remain usable. For reasons of security, there is one thing administrators cannot do as with other systems: They cannot retrieve the password of a user in plaintext. But, of course, they can reset it.

The exclusively administrator controlled functions are managed by a local tool within the VPN, as is indicated by *GDS-Admin* in Figure 1. It offers the following functions to administrators:

- Creation of a user and assignment of the initial object set. If this is a new set, it must be created also to complete the creation of that user. For temporary users, the given start and end times are checked for plausibility: The start time must not be in the past and must be earlier than the end time.
- Alteration of user data.
- Deletion of a user. This requires that he does not possess any object sets. It implies removal from all groups the user was a member of.
- Creation and deletion of a group.
- Addition of a user to a group.
- Deletion of a user from a group.

The following further functions are available to administrators locally and remotely as a service for common users. If used by an administrator they can be applied to any user, but an ordinary user can perform them only on own data objects, objects sets, memberships, or user data. As this restriction is valid for all functions below, it is not repeated for reasons of linguistic simplicity:

- Granting, deleting, or changing access rights to an object set for a group.
- Changing of access rights of an owner to his object sets.
- Creation and deletion of an object set. Only empty object sets are erasable. For a newly created object set owner access rights must be given.
- Transfer of the ownership of an object set to another user.
- Transfer of data objects to another object set. If applied by an ordinary user, he must be the owner of the source object set.
- Listing functions for users and groups and their access rights.
- Change of a password.

3.5.5 User and Rights Administration

As pointed out above, the management of the VPN and GDS users is completely separated from the user management of the IT infrastructure which hosts both VPN and GDS. The list of VPN users, the TACACS$^+$-server relies on is generated by the user administration tool of the GDS. Therefore, the services of GDS can be used only by users, who have authenticated themselves before access was granted. Furthermore, the administration tool itself can be accessed locally only. We think that the overall security is further enhanced by these measures.

4 CURRENT IMPLEMENTATION

Figure 2 shows the current prototypic implementation, which at present is mainly used to manage data objects generated by the EDRs. In the future, also data of the Electrical Grid Analysis Simulation Modeling and Visualization Tool (*e*ASiMoV), see (Maaß *et al.,* 2012), (Maaß *et al.,* 2014) will be managed. The VPN is realized using a Cisco router, mainly because we have an existing infrastructure based on Cisco hardware and the respective licences and everything else would be more expensive. Nevertheless, other manufacturers like Juniper or Checkpoint can be used alternatively, of course. At present, we use one Cisco ASA 5505 with a back-up device of the same type in cold

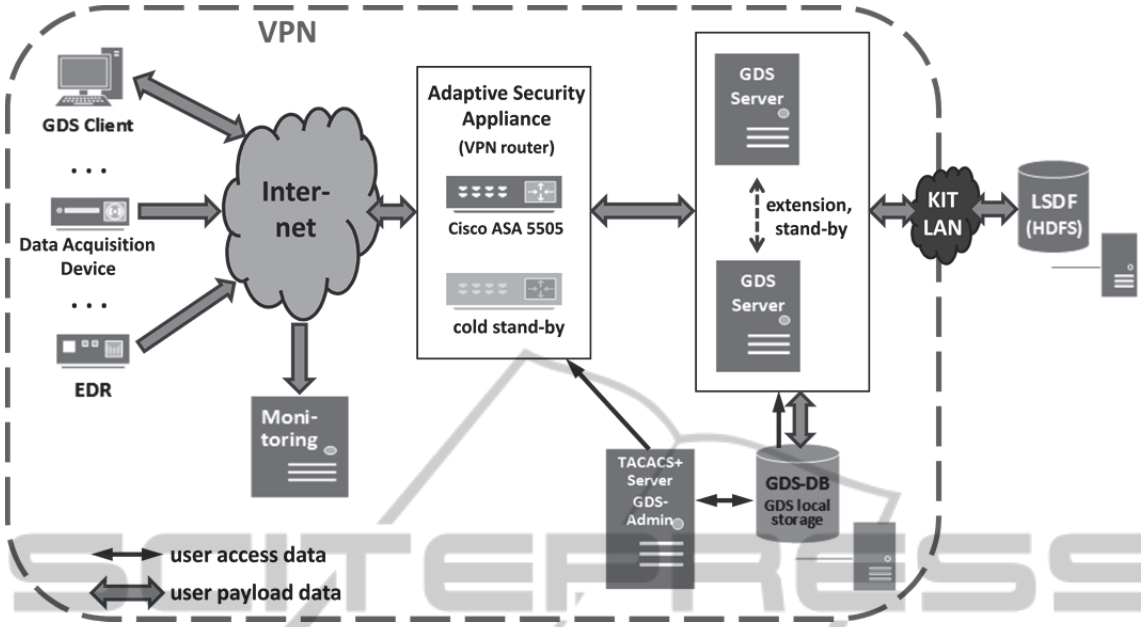

Figure 2: First implementation of the SeGDS concept based on one active Cisco ASA 5505 and six parallel GDS servers. A second ASA is available as cold stand-by to replace the active one in case of a breakdown. For cost reasons, the LSDF is connected through the KIT LAN.

stand-by. Unfortunately, this is a bottleneck due to a limited budget for the prototype.

The main structural difference to the concept shown in Figure 1 is that the HDFS file server is accessed via KIT LAN outside of the VPN, which is done mainly for cost reasons. This solution is justifiable as long as the stored data are pseudonymized, as it is the case with the EDR data. The planned integration of a GPFS file server will be done more securely via ssh or scp and/or within the VPN.

There is a special client called *Monitoring*, which was added to the current implementation. It is based on RDP (Remote Desktop Protocol) and serves as a tool for supervising the EDRs. A list of connected EDR devices, including performance information about the acquisition hardware and data transfer, is created. If necessary, EDRs can be restarted. Since the monitoring is only used within the VPN, the known security weaknesses of RDP can be accepted at this stage of application. The monitoring tool helps to detect malfunctions of the EDRs and to fix them by restarting also from outside of the KIT campus.

5 SUMMARY AND OUTLOOK

We have given a list of criteria for a secure, reliable, scalable, and generic data exchange and management system and demonstrated how they can be met by standard solutions. The preference of standard solutions results in both, comparably low prices and synergy effects with other applications in terms of technical development and new standards and the discovery of vulnerabilities and their elimination. An overall concept of the secure generic data services was given and a first prototypic implementation was introduced.

Future development will concentrate on the secure integration of a GPFS file server. It is also planned to enlarge the VPN so that more clients can be added and the communication to the LSDF is integrated. Parallel to that, the robustness of the security measures will be tested by supervised intrusion attacks. The quality of the approach will be investigated in various performance-tests.

REFERENCES

Bach, F., Çakmak, H.K., Maaß, H., Kuehnapfel, U., 2012. Power Grid Time Series Data Analysis with Pig on a Hadoop Cluster Compared to Multi Core Systems. In: Stotzka, R., Milligan, P., Kilpatrick, P., eds. *21st*

Euromicro International Conference on Parallel, Distributed, and Network-based Processing, 27 Feb - 1 Mar 2013, IEEE, Piscataway, N.J, 208–212.

Bakken, D., Bose, A., Hauser, C., Whitehead, D., Zweigle, G., 2011. Smart Generation and Transmission With Coherent, Real-Time Data. *Proceedings of the IEEE,* 99 (6), 928–951.

Berger, L.T., Iniewski, K., 2012. *Smart grid. Applications, communications, and security*, Wiley. Hoboken, N.J.

Grid Security - Industry Solutions, 2011 [online]. Cisco Systems. Available from: http://www.cisco.com/web/strategy/energy/smart_grid_security.html [Last update 1 January 2011] [Accessed 13 May 2014].

Doraswamy, N., Harkins, D., 2003. *IPSec. The new security standard for the Internet, intranets, and virtual private networks*, Prentice Hall PTR. Upper Saddle River, NJ, 2nd ed.

ENISA, ed., 2012. *Smart Grid Security. Annex II: Security aspects of the smart grid.* ENISA (European Union Agency for Network and Information Security). Available from: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations [Accessed 14 April 2014].

Eckert, C:., 2012. *IT-Sicherheit*, (in German) Oldenbourg Verlag, München.

Fed. Min. of Economy and Energy, 2012. *E-Energy: Startpage* [online]. Federal Ministry of Economic Affairs and Energy, Germany. Available from: http://www.e-energy.de/en/ [Accessed 23 April 2014].

Ferguson, N., Schneier, B., Kohno, T., 2010. *Cryptography engineering. Design principles and practical applicationns*, Wiley. Indianapolis.

García, A., Bourov, S., Hammad, A., van Wezel, J., Neumair, B., Streit, A., Hartmann, V.; Jejkal; Neuberger; Stotzka, 2011. The Large Scale Data Facility: Data Intensive Computing for Scientific Experiments. In: *25th IEEE International Symposium on Parallel and Distributed Processing (IPDPS 2011)*, 16-20 May 2011, IEEE, Piscataway, NJ, 1467–1474.

IBM and Alliance - Energy and utilities solutions from IBM and Juniper Networks - United States, 2014 [online]. IBM Corporation. Available from: http://www.ibm.com/solutions/alliance/us/en/index/juniper_energy.html [Last update 8 May 2014] [Accessed 13 May 2014].

Smart Grid Experts, Information, News & Conferences, 2014 [online]. IEEE. Available from: http://smartgrid.ieee.org/ [Accessed 13 May 2014].

Energy and Utilities - Smart Grid Security Solution, 2014 [online]. Juniper Networks. Available from: http://66.129.228.18/as/en/solutions/enterprise/energy-utilities/ [Accessed 13 May 2014].

Li, F., Luo, B., Liu, P., 2011. Secure and privacy-preserving information aggregation for smart grids. *International Journal of Security and Networks,* 6 (1), 28-39.

Maaß, H., Çakmak, H.K., Bach, F., Kuehnapfel, U., 2014. Preparing the Electrical Data Recorder for Comparative Power Network Measurements. In: . *IEEE International Energy Conference and Exhibition (ENERGYCON)*, 13-16 May 2014, IEEE, Piscataway, NJ.

Maaß, H., Çakmak, H.K., Süß, W., Quinte, A., Jakob, W., Stucky, K.-U., Kuehnapfel, U.G., 2012. Introducing the Electrical Data Recorder as a new capturing device for power grid analysis. In: *IEEE Applied Measurements for Power Systems (AMPS)*, 26-28 Sep 2012, IEEE, Piscataway, NJ, 1–6.

Menezes, A.J., van Oorschot, P.C., Vanstone, S.A., 1997. *Handbook of applied cryptography*, CRC Press. Boca Raton.

Mlynek, P., Misurec, J., Koutny, M., Raso, O., 2013. Design of secure communication in network with limited resources. In: . *4th IEEE/PES Innovative Smart Grid Technologies Europe (ISGT EUROPE)*, 6-9 Oct 2013, IEEE, Piscataway, NJ, 1–5.

NIST, 2014. *SHA-3 Standardization* [online]. National Institute of Standards and Technology (NIST), Computer Security Division. Available from: http://csrc.nist.gov/groups/ST/hash/sha-3/sha-3_standardization.html [Last update 7 April 2014] [Accessed 12 May 2014].

Oppliger, R., 2009. *SSL and TLS. Theory and practice*, Artech House. Boston.

Partida, A., Andina, D., 2010. *IT security management*, Springer. Dordrecht, London.

Rescorla, E., 2000. *SSL and TLS. Building and designing secure systems*, Addison-Wesley. Harlow.

Stallings, W., 2013. *Network security essentials. Applications and standards*, Prentice Hall. Upper Saddle River, NJ.

Stucky, K.-U., Süß, W., Çakmak, H.K., Jakob, W., Maaß, H., 2014. Generic Data Management Services for Large Scale Data Applications. *to be published*.

U.S. Dept. of Energy, 2014. *Home | SmartGrid.gov* [online]. U.S. Department of Energy. Available from: https://www.smartgrid.gov/ [Last update 22 April 2014] [Accessed 23 April 2014].

Yu, T., Jajodia, S., eds., 2007. *Secure data management in decentralized systems*. New York, Springer.