Secure Cloud Reference Architectures for Measuring Instruments under Legal Control

Alexander Oppermann[1], Jean-Pierre Seifert[2] and Florian Thiel[1]
[1]*Physikalisch-Technische Bundesanstalt (PTB), Berlin, Germany*
[2]*Security in Telecommunications, Technische Universität Berlin, Berlin, Germany*
{*alexander.oppermann, florian.thiel*}*@ptb.de, jpseifert@sec.t-labs.tu-berlin.de*

Keywords: Cloud Computing, Trusted Cloud, Homomorphic Encryption, PKI, Verified Computing, Legal Metrology.

Abstract: Cloud Computing has been a trending topic for years now and it seems it has finally become mature enough for widespread commercial application. In this paper, the authors describe their approach to establish a secure cloud architecture which conforms to the Measuring Instruments Directive of the European Union while keeping the flexibility and benefits that cloud computing promises for companies and customers alike. The authors introduce a modular concept of a secure cloud system architecture which will ensure cross-virtual machine collaboration and a legitimate, secure and protected flow of measurement data.

1 INTRODUCTION

Cloud computing is growing steadily in Europe from 17.2 billion Euros in 2015 to 44.8 billion Euros by 2020 (Bradshaw et al., 2014). In Germany its growth amounted to around 46% from 2013 to 2014, which correlates to a volume of 6.4 billion Euros (Bitkom, 2014). Bitkom further predicts that by 2018 the market will grow to a total volume of 19.8 billion Euros in Germany alone. This prediction and the actual development seem to correlate with Gartner's Hype Cycle (Rivera and Van der Meulen, 2014) where Cloud Computing has been placed in the trough of disillusionment (see Figure 1). However, in 2015 the same analysts concluded that Cloud Computing left the Hype Cycle (Rivera and Van der Meulen, 2015) and should be considered a widely accepted and adopted technology.

The main reason for the success of Cloud Computing is that the total up-front-investments needed to run traditional IT infrastructure can be significantly reduced. In particular small and medium-size enterprises (SME) can profit from more transparent cost-schemes and cost-savings for maintaining up-to-date and especially secure IT infrastructure.

The market under legal control, i.e. gas meters, electricity meter, petrol pumps, etc., has an annual turnover of 104 to 157 billion Euro in Germany (Leffler and Thiel, 2013). And, of course, the manufacturers of these measuring instruments also want to present their customers with modern interconnected

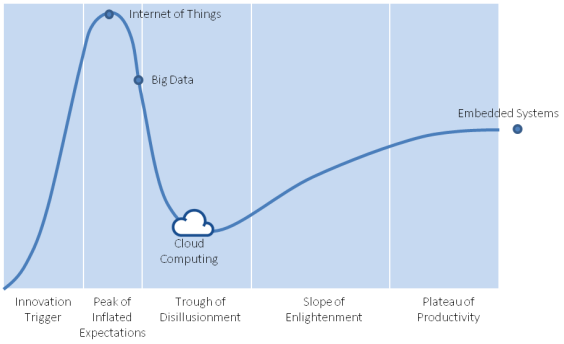

Figure 1: Gartners Hype Cycle from 2014 (Rivera and Van der Meulen, 2014). Including embedded systems which are already off the chart.

"cloud ready" devices, which will increase their comfort in dealing with them through e.g. new services for mobile devices.

However, one has to make sure that these new type of measuring instruments are as secure as their classical counterparts, since constructing a secure measuring instrument which is always connected to an insecure network is quite challenging and very complex. Further with the use of cloud computing the aggregation of data is inevitable, but these huge amounts of potentially profitable data will attract new attackers. The assurance of correct measurements and consumer protection are the highest priorities when working in the area of legal metrology. Each measuring instrument has to fulfill the legal requirements and, in addition, has to be secure against tampering and inten-

Oppermann, A., Seifert, J-P. and Thiel, F.
Secure Cloud Reference Architectures for Measuring Instruments under Legal Control.
In *Proceedings of the 6th International Conference on Cloud Computing and Services Science (CLOSER 2016) - Volume 1*, pages 289-294
ISBN: 978-989-758-182-3

tional as well as unintentional manipulation.

The interfaces in classical measuring instruments could be easily sealed and hence trust was easily established. Nowadays, with cloud applications and services, hardware-based seals are useless against software-based interfaces. One has to find new ways to establish trust in such systems.

The remainder of this paper is organized as follows: Section 2 gives an overview on how legal metrology is organized; Section 3 gives an outlook of how a secure cloud architecture can be achieved and describes homomorphic encryption; Section 4 describes related works; Section 5 gives a brief description of the research scenarios and its benefits for legal metrology.

2 LEGAL METROLOGY

Legal metrology covers a wide range of measuring instruments from those with commercial or administrative purposes to those intended for public interests. In Germany over 100 million legally relevant meters are in use (see (Leffler and Thiel, 2013)). The vast majority of them are employed for business purposes, like commodity meters in the fields of water, gas, electricity or heat. Furthermore, common applications for meters are petrol pumps or scales in e.g. super markets. The traffic system, for example, requires large amounts of meters for speed and alcohol, in order to guarantee safety. All of these applications have in common the fact that neither the user nor the affected person can check the validity of the determined result. Instead they rely on the accuracy of the official measurement and calibration of these measuring instruments. The key purpose of legal metrology is to assure the correctness of measurements and further to enhance public trust in them. Additionally, legal metrology fulfills the need to ensure the functioning of the economic system while protecting the consumer at the same time.

The *International Organization of Legal Metrology* (OIML) was founded with the aim to harmonize regulations across national boundaries worldwide and to avoid trade barriers due to legal requirements. The document OIML D 31 (de Métrologie Légale, 2008) focuses especially on software requirements for legal measuring instruments (cf. (Kochsiek and Odin, 2001)).

WELMEC is the European committee responsible for harmonizing legal regulations in the area of legal metrology. The committee publishes guides and supports notified bodies (public or private organized departments to verify measurements devices) throughout Europe and manufacturers alike, which implement the Measuring Instruments Directive (MID) (cf. (Kochsiek and Odin, 2001), (Peters et al., 2014)).

2.1 Measuring Instrument Directive

The Measurement Instrument Directive (MID) is based on two European directives (2014/32/EU, 2014) (2004/22/EC, 2004), the latter will be replaced by the first this year. These directives aim for the harmonization and establishment of common European standards for measuring instruments. Aside from this, the MID is designed to enable fair trade and trust in the public interest as well as to protect the consumer.

The MID comprises ten types of measuring instruments that are of special interest and importance to the economy due to their wide-spread or cross-border use. These are: water meters, gas meters and volume conversion devices, active electrical energy meters, heat meters, measuring systems for the continuous and dynamic measurement of quantities of liquids other than water, automatic weighing instruments, taximeters, material measures, dimensional measuring instruments, and exhaust gas analyzers. In the annex of the directive there are definitions, fault tolerances and specific requirements outlined for each type of the prior mentioned measurement instruments. The specific requirements involve, e.g. basic tamper protection and a display for measurement data.

Before putting a new measuring instrument on the market, the manufacturer has to declare the conformity with the MID based on the assessment by a Notified Body in Europe (cf. Figure 2). The *Physikalisch-Technische Bundesanstalt (PTB)* is a Notified Body in Germany. Aside from that role, the PTB is the German national metrology institute and acts as an interface between scientific research and economic interests. Furthermore, the PTB is responsible for technical expertise related to measuring instruments, conformity assessment, monitoring of product related quality assurance systems and advising with European regulations. Given the scope of these responsibilities, it is crucial that the Notified Body be independent and neutral in order to be able to fulfill its duties impartially.

2.2 WELMEC

The European Free Trade Association (EFTA) and European Cooperation in Legal Metrology are responsible for WELMEC. At the moment 37 countries are part of the WELMEC Committee. The committee has established eight WELMEC Working Groups (WG) with WG7 in charge of software

matters and distributing the *WELMEC 7.2 Software Guide*. The current version is WELMEC 7.2 Issue 5 (WG7, 2012). In the near future Issue 6 will be released.

The WELMEC 7.2 Software Guide gives an overview of software security with a special focus on measuring instruments. Furthermore, it helps manufacturers and Notified Bodies alike by providing examples and rules on how to achieve software security, which guarantee compliance with the software related part required by the MID, if followed.

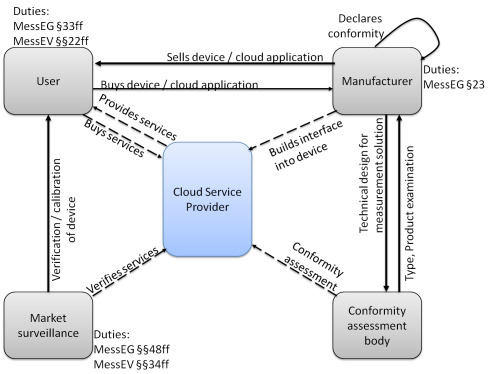

Figure 2: Overview of the different actors their roles, schedule of responsibilities and duties in legal metrology. The cloud service provider role has to be determined.

When designing software for secure measuring instruments it is advisable to isolate the legally relevant part from the legally non-relevant one. Likewise, the non-relevant part may not influence the legally relevant one. This may be realized by means of protected interfaces. Moreover, if the software is modular it will ease the update process for manufacturers and Notified Bodies. Legally relevant modules are defined by WELMEC 7.2 Software Guides as modules that make contributions to or influence measurement results. Examples include displaying data, protecting data, saving data, identifying the software, executing downloads, transferring data, and checking of received or stored data (cf. (WG7, 2012).

3 SECURE CLOUD ARCHITECTURE

Cloud Computing has its antecedents in several different concepts like mainframes, client/server computing, peer-to-peer distributed computing, collaborative computing and grid computing in general. In the end, the essence of cloud computing can be summed up in one slogan from Sun Microsystem “The network is the computer” (c.f. (Miller, 2008)).

Thus, most security threats within cloud computing are neither new nor unknown to security experts but can be dealt with through traditional security processes and mechanisms like security policies, identity management (IAM), intrusion detection/prevention systems, cryptography and vulnerability analysis systems (e.g. OpenVAS) (cf. (Hogan et al., 2011).).

When using a cloud computing solution one also has to consider that large amounts of data will be accumulated in one place and thus become a more attractive target for information retrieval be it legal or non-legal. The robustness and redundancy of the infrastructure has to be one of the main aspects of a secure reference architecture for cloud computing. It is also important to match the threat model with the real world while creating and determining the requirements for a cloud architecture.

In legal metrology the role of a benevolent system administrator does not exist and therefore every party has to be distrusted from the beginning. This fact leads to interesting and challenging use cases which make this field exceptionally interesting from a security point of view. If the service technician and administrator of a cloud service provider are considered untrustworthy, then data integrity, data security and eventually data privacy are very difficult to guarantee. One can argue that with classical cryptography all these issues can be solved. But instead of presenting a solution one will avoid these problems. The benefits of using cloud computing will be invalid, because the user has to download the data and decrypt them locally in order to be able to process the data. The reason to store the data in the cloud in the first place would then be nullified. The authors plan to counter this problem with fully homomorphic encryption (FHE).

3.1 Homomorphic Encryption

In 1978 Rivest, Adleman and Dertouzos introduced along with the prior invented crypto system RSA (Rivest et al., 1978b) the possibility of homomorphic encryption (Rivest et al., 1978a). Homomorphic Encryption allows operation on encrypted data without decrypting it first. In 2009 Gentry was able to show that a crypto system exists which obtains both properties. He introduced the first fully homomorphic crypto system to the world based on ideal lattices (Gentry et al., 2009). In 2010 Gentry published an optimized version of this system using only modular arithmetic to construct a fully homomorphic scheme from a “bootstrappable” somewhat homomorphic scheme (c.f. (Van Dijk et al., 2010)).

3.1.1 Classification of Homomorphic Schemes

Armknecht et al. presented some attributes (correctness for decryption and evalution, compactness) of homomorphic encryption schemes, in order to be able to classify the different schemes correctly, since all homomorphic schemes do not share the same properties. A scheme consists of generating the keys (Gen), encryption (Enc), evaluation of the ciphertext (Eval) and Decryption (Dec). They determined three classifications, but this paper focus only on the main two:

A *Somewhat Homomorphic* scheme (Gen, Enc, Eval, Dec) has to have correct decryption and correct evaluation. For compactness no rule is set, so that the ciphertext can increase in length with each homomorphic operation.

A *Fully Homomorphic* scheme (Gen, Enc, Eval, Dec) has to be compact, correct and the scheme itself is a set of all circuits. This leads to that the scheme can evaluate any circuit of whichever size.

3.1.2 Approach using Fully Homomorphic Encryption

The authors use fully homomorphic encryption within the measuring instrument and send the encrypted measuring data to the cloud, in order to be able to ensure data security and integrity (see Figure 3). Working on encrypted data reduces the attack vectors enormously. A malicious insider cannot change the data easily, nor can a VM spy on the processed data. Using this technology enables the platform to reduce the biggest attack vectors for cloud computing. Further, it avoids particular requirements for ”cloud ready” measuring instruments and the need to deploy special hardware for servers in order to enable trust and security in a cloud computing platform.

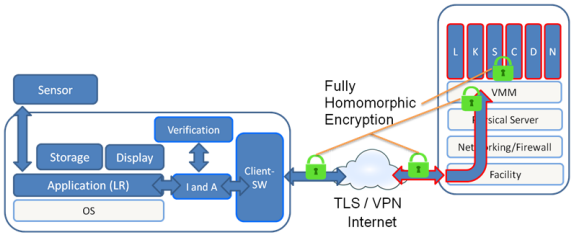

Figure 3: Legal Cloud Framework: Measurement Device and Cloud Architecture secured via TLS and homomorphic encryption. L: Legally relevant VM, K: Key & Signature Manager, S: Storage Manager, C: Connection Manager, D: Download Manager, N: legally non-relevant VM.

3.1.3 Problems with Homomorphic Encryption

Despite the popularity of homomorphic encryption, most homomorphic encryption schemes exist on paper (Armknecht et al., 2015) rather than as implemented systems. Furthermore, the computation time is still a big issue. Nevertheless some interesting implementations are available and will be evaluated, like HElib, FHEW, HomomorphicEncryption R Package (Aslett et al., 2015) and NTRU based implementation (see (Rohloff and Cousins, 2014)). Elaborating these schemes will be part of the authors future research work (see section 6).

4 RELATED WORK

This section gives a brief overview of recent related work, which addresses similar challenges in different domains.

4.1 SensorCloud

The project’s main objective is to guarantee user control of the data once submitted it into the cloud. The focus thus lies on sensor data in general. The proposed cloud architecture enforces end-to-end data access control over a well-defined entry-point which provides end-to-end data protection, due to encryption and integrity protection (Catrein and QSC AG, 2013).

4.2 Sealed Cloud

This research project proposes an architecture which will safeguard the data and meta-data within the cloud and protect it against insider attacks by a system administrator. If an administrator tries to access the server physically, the system will shutdown first and delete all data, so that the administrator will not be able to access the data or even data fragments in memory. In addition, a chain of trust via a hardware based TPM-module will be built and thus can check the system integrity from the beginning of the boot process (Jäger et al., 2013).

4.3 TRESOR

TRESOR is a cloud infrastructure research project which is developed by TU Berlin and is dedicated to secure electronic patient data (e-health) in a hospital, which then can be accessed by various doctors for the benefit of the patient’s health. The project developed a cloud platform which provides several cloud-services, the most important of which are a cloud-broker to access these services and a cloud-proxy to monitor the control of cloud usage (c.f. (Slawik et al., 2012)).

5 RESEARCH SCENARIOS

This section discusses the research scenarios which were developed and shaped by the needs of manufacturers and the requirements of legal metrology. The focus of these scenarios are clearly on SME's which are planning to move their products into the cloud but have to balance their openness with security risks and innovation cycles. The drafted models may appear conservative, but this is because they are the result of a short term view to enable SME's to take the leap to the next level of computing and innovation. From there the aim is to facilitate the whole spectrum of the cloud possibilities, like using hybrid cloud, or elaborating concepts like cloud bursting, and finally moving to public clouds in order to reduce costs significantly.

5.1 Virtualized Measuring instrument

This scenario is the most ambitious one, since there is only the sensor and the data acquisition left with the rest moved to the cloud. This means, of course, that one has to sign the data securely, in order to guarantee its integrity before it is sent to the cloud. The processing, storage and the other services, legally relevant or not, will be run separately from each other in virtual machines. The display is detached from the measuring instrument like in the following scenarios. Thus, the data can be accessed by the permitted market participants from everywhere. This scenario will reduce the costs significantly for measuring instruments, but is the most challenging when trying to achieve conformity with the MID at the moment.

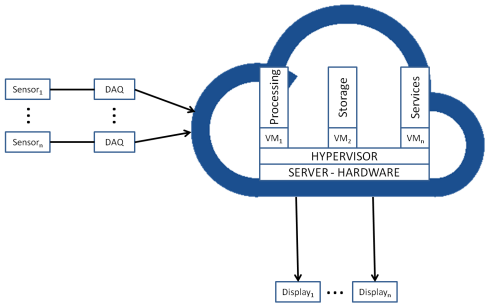

Figure 4: Research Scenario: Fully virtualised measuring instrument moved to the cloud.

5.2 Data Export

The sensor measures the real-world data and the measurement instrument acquires all the data produced by the sensor. Then the acquired data will be processed within the measuring instrument and the calculated result will be signed cryptographically and sent to the cloud, where it will be securely stored. Now only permitted market participants are able to access the data and can display them on their device. If a secure display is needed the integrity of the data can be assured via the cryptographically secured hashes. This scenario is in accordance with the German Verification Act (Mess- und Eichgesetz/Mess- und Eichverordnung (MessEG/EV)), since all the processing will be done in a calibrated device. To assure the security of the processed data against tampering, it will be signed before leaving the secured environment.

5.3 Algorithm and Parameter Export

In this scenario the sensor measures the real-world data and passes it to the measuring instrument, where it will be acquired. Before processing the data, the measuring instrument has to connect to the cloud and will load the specific algorithm and necessary parameters, in order to execute the processing of the acquired data locally. The result will be passed on to a display. While designing this scenario, the goal was to protect the intellectual property of the manufacturers, who want to produce their hardware in non-secure environments and cannot protect themselves against imitations. So in short, the measuring instrument itself is a *dumb* device and the intelligence is outsourced into the network.

A slightly different approach for this scenario is to divide the software modules into legally relevant and non-legally relevant software. Now the processing of the legally relevant part will be done locally in the calibrated measuring instrument and then the result will be pushed into the cloud, where the non-legally relevant part of the software is stored. From the cloud the processed data can be accessed together with the non-legally relevant attributes.

6 CONCLUSIONS AND FUTURE WORKS

In this paper a brief overview of the special field of legal metrology and its unique requirements for measuring instruments were given. The authors took the foundation of Daniel Peters' previous work (Peters et al., 2015) which already fulfills most requirements of the MID and the WELMEC 7.2 Software Guide. It was the initial work in the field of virtualization in legal metrology. This research work identified different needs of the cloud platform and will expand as well as alter the framework to fit legal requirements on its

highest protection level, in order to benefit from the technical advantages of the cloud computing solution.

The next steps will be to configure an Openstack Cloud and to implement that framework. In addition, the feasibility of the proposed framework has to be proven and its performance and robustness against standard attack vectors has to be measured.

Furthermore, the prior mentioned different homomorphic encryption schemes have to be elaborated and practically implemented into the framework. With the help of FHE, the authors will be able to secure data and algorithms against manipulation within the cloud. The performance for encryption, decryption and function execution on encrypted data have to be measured. Lastly, a risk analysis of the platform will be performed, as it will be required by the MID (Esche and Thiel, 2015).

REFERENCES

2004/22/EC, D. (2004). Directive 2004/22/EC of the European Parliament and of the Council. *Official Journal of the European Union*.

2014/32/EU, D. (2014). Directive 2014/32/EU of the European Parliament and of the Council. *Official Journal of the European Union*.

Armknecht, F., Boyd, C., Carr, C., Gjøsteen, K., Jäschke, A., Reuter, C. A., and Strand, M. (2015). A guide to fully homomorphic encryption.

Aslett, L. J. M., Esperança, P. M., and Holmes, C. C. (2015). A review of homomorphic encryption and software tools for encrypted statistical machine learning. Technical report, University of Oxford.

Bitkom (2014). Markt für Cloud Computing wächst ungebrochen.

Bradshaw, D., Cattaneo, G., Lifonti, R., and Simcox, J. (2014). Uptake of cloud in europe - follow-up of idc study on quantitative estimates of the demand for cloud computing in europe and the likely barriers to take-up. *Digital Agenda for Europe*.

Catrein, D. and QSC AG, C. (2013). Maintaining user control while storing and processing sensor data in the cloud. *International Journal of Grid and High Performance Computing*, 5(4):97–112.

de Métrologie Légale, O. I. (2008). General requirements for software controlled measuring instruments.

Esche, M. and Thiel, F. (2015). Software risk assessment for measuring instruments in legal metrology. In *Computer Science and Information Systems (FedCSIS), 2015 Federated Conference on*, pages 1113–1123. IEEE.

Gentry, C. et al. (2009). Fully homomorphic encryption using ideal lattices. In *STOC*, volume 9, pages 169–178.

Hogan, M., Liu, F., Sokol, A., and Tong, J. (2011). Nist cloud computing standards roadmap. *NIST Special Publication*, 35.

Jäger, H. A., Monitzer, A., Rieken, R. O., and Ernst, E. (2013). A novel set of measures against insider attacks-sealed cloud. page 187.

Kochsiek, M. and Odin, A. (2001). Towards a global measurement system: Contributions of international organizations. *OIML Bulletin*, 42(2):14–19.

Leffler, N. and Thiel, F. (2013). Im Geschäftsverkehr das richtige Maß - Das neue Mess und Eichgesetz, Schlaglichter der Wirtschaftspolitik. *Monatsbericht; Bundesministerium für Wirtschaft und Technologie (BMWi)*.

Miller, M. (2008). *Cloud computing: Web-based applications that change the way you work and collaborate online*. Que publishing.

Peters, D., Grottker, U., Thiel, F., Peter, M., and Seifert, J.-P. (2014). Achieving software security for measuring instruments under legal control. In *Federated Conference on Computer Science and Information Systems pp. 123–130*.

Peters, D., Peter, M., Seifert, J.-P., and Thiel, F. (2015). A secure system architecture for measuring instruments in legal metrology. *Computers*, 4(2):61–86.

Rivera, J. and Van der Meulen, R. (2014). Gartner's 2014 hype cycle for emerging technologies maps the journey to digital business. *Retrieved March*, 31:2015.

Rivera, J. and Van der Meulen, R. (2015). Gartner's 2015 hype cycle for emerging technologies maps the journey to digital business. *Retrieved March*.

Rivest, R. L., Adleman, L., and Dertouzos, M. L. (1978a). On data banks and privacy homomorphisms. *Foundations of secure computation*, 4(11):169–180.

Rivest, R. L., Shamir, A., and Adleman, L. (1978b). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126.

Rohloff, K. and Cousins, D. B. (2014). A scalable implementation of fully homomorphic encryption built on ntru. In *Financial Cryptography and Data Security*, pages 221–234. Springer.

Slawik, M., Zickau, S., Thatmann, D., Repschläger, J., Ermakova, T., Küpper, A., and Zarnekow, R. (2012). Innovative architektur fur sicheres cloud computing: Beispiel eines cloud-ecosystems im gesundheitswesen.

Van Dijk, M., Gentry, C., Halevi, S., and Vaikuntanathan, V. (2010). Fully homomorphic encryption over the integers. In *Advances in cryptology–EUROCRYPT 2010*, pages 24–43. Springer.

WG7 (2012). Welmec 7.2 issue 5 software guide. *WELMEC Euro- pean cooperation in legal metrology*.