Trustworthy Evidence Gathering Mechanism for Multilayer Cloud Compliance

Markus Florian
University of Applied Sciences
Wr. Neustadt, Austria
Email: 80166@fhwn.ac.at

Sarita Paudel
Vienna University of Technology
Vienna, Austria
Email: e1029083@student.tuwien.ac.at

Markus Tauber
Austrian Institute of Technology
Vienna, Austria
Email: Markus.Tauber@ait.ac.at

***Abstract*—Cloud Computing allows the designing of systems which dynamically acquire compute resources. This makes it very suitable for Critical Infrastructures where unpredictable load due to human usage patterns are very likely. Especially in this domain legal compliance is a growing concern in general. Abstraction over multiple architectural cloud layers allows for individual layers being operated by different providers. This makes it hard to determine whether legal compliance is given. In this paper we motivate the research towards an *Event Gathering Mechanism* which is envisioned to allow the modelling of legal aspects in a multi layered cloud environment.**

***Keywords*—Cloud; Critical Infrastructure; Techno-Legal**

I. Introduction

Critical Infrastructures (CI) provide essential utilities like water supply, electricity or transportation. Such infrastructures need to cope with variable usage, high flexibility and fail-overs to work properly. Modern IP based CI control systems allow more efficient control than traditional systems. The variable workload, unpredictable usage spikes and outsourcing of data handling, make the Cloud interesting for CI IT. Another advantage of using the Cloud in this context is to aggregate data from the IP enabled control devices which have limited resources and cannot process data locally. This means that sooner or later CI providers will use cloud applications for their systems and hence related issues need to be investigated. Especially with CI in the Cloud, legal compliance is very important and hence the chosen focus of this work. CI data is normally highly sensitive and therefore subject to legal regulations for data security. Traditional CI secured the data inside a closed environment without or with extremely restricted external access. Thus making it really important to establish a data access regulations to secure CI-data inside the Cloud. Additionally CI clients often lack the possibility of performing adequate logging or security tasks due to the lack of resources.

Cloud usage allows various business models - e.g. Software As A Service (SAAS) which provides e.g. an elastic application abstracting completely about the underlying hardware or infrastructure whereas an Infrastructure As A Service (IAAS) model provides virtualized instances of operating systems. A typical cloud service is not limited to include an individual provider, for example a SAAS provider can be customer of an IAAS provider. Therefore, it is important that not only actions inside the CI Provider's virtual address space, i.e. the IAAS cloud application, are logged and at his disposal to detect misuse of the data and to trigger countermeasures or to proof lawful handling and legal compliance of the data handling. In the case where a CI cloud application is operated as SAAS, information may be required (e.g. geo-location) which is only available to the IAAS layer.

To address these issues we propose an advanced logging facility which we name *evidence gathering mechanism (EGM) for a multilayer cloud environment* as shown in Fig 1. Our EGM is planned to gather and distribute logging information to corresponding subscribers. It provides interfaces between the different cloud layers and subscribers to which every event inside the corresponding cloud layer needs to be sent. To guarantee legal compliance it should also be able to model legal requirements supporting both, data protection and Service Level Agreements (SLA)[1] which may vary between layers. Our contribution beyond this paper is to combine legal and technical aspects in cloud computing and to provide means for CI providers to use cloud applications under considerations of their legal requirements which may be more stringent than those of common commercial applications. The goal of this paper in particular is to motivate this work and to provide an overview of gabs in related work.[1]

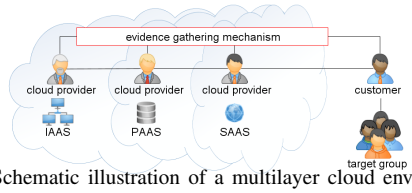

Figure 1. Schematic illustration of a multilayer cloud environment, with a CI provider as customer, including the evidence gathering mechanism.

II. Related Work

We summarize the general situation by stating that to the best of our knowledge existing logging facilities and cloud security mechanisms only provide Service Level Agreement (SLA) compliance or IAAS logging and lack the possibility of transparency in a multilayer cloud structure.

P. Sudhakar[2] suggests a Cloud Information Accountability (CIA) Framework not only for logging but also for protection purpose. He proposes a JAR-wrapper for every information stored inside the Cloud which handles authentication for access and logging. The log files produced inside the JAR archive are then periodically sent to the data owner. This procedure ensures that every copy of the archive shares the same security level and logs its access. The for CI additionally required multilayer transparency and modelling of the legal aspects is not considered in this Framework.

S. Chen and C. Wand[3] propose accountable cloud systems and discuss how evidence can be stored and provided to

[1]This work is supported by *SEcure Cloud computing for CRitical infrastructure IT (SECCRIT)* – an EU FP7 project (Contract Nbr. 312758).

identify the owner of the problem. They operate in different domains. They suggest to provide accountability as a service outside of the observed system to increase the security and accountability of the logged information. Their logging template is designed to work as an insurance between different business partner in a collaborated business process. In theory this schema could be applied for a multilayer cloud system but the system is only in action between defined business partner and in defined business processes. To propose a more general approach and provide a higher degree of security the desired solution should be integrated into the cloud system instead of separated and outsourced into its own cloud.

Multiple works [4][5] state examples for gathering location information for data to comply locational restrictions inside SLA's. In legal aspects this information may also be relevant. Legal regulations expect the operator of the cloud application to provide his costumers with the information of which data are how and where processed and stored. Therefore the operator needs to know in which countries the physical storage resides. The locations are agreed upon in SLA's and verified through data provided by methods like mentioned above. But with only IAAS as the considered CI these approaches are to specifically defined as to use them in a multilayer cloud environment without adoption.

A Generic Logging Template for IAAS Cloud[6] lists the main threats in combination with outsourcing into the Cloud and provides a generic logging template to identify the problems and reduce the impact. However the template is simplified and only one cloud provider is assumed. Furthermore the service sold is IAAS. To completely comply with the law a general assumption for every possible cloud structure must be made.

Cloud Log Forensics Metadata Analysis[7] highlights the re-usability of the hypervisor log file and its metadata for digital forensics but gives no indication on how to obtain these information without complete access to the system.

Traditional CI ensures security, access regulation and logging through infrastructure[8]. This solutions, suggestions and frameworks could be adapted into the Cloud but would leave some security issues open. Additionally because of the solution being based on Infrastructure, only IAAS Customers could possible establish these measures.

III. EVIDENCE GATHERING MECHANISM

To cope with the lack of transparency an evidence gathering mechanism is proposed. It's intended functionality can be divided into three categories: (i) Data gathering, (ii) Metric matching and (iii) Data distribution. The data gathering process supplies raw logging data while the metric matching algorithm provides situational data conclusions. The data distribution takes care of delivering the information so the data can be stored as evidence.

(i) Data gathering: To acquire information of what is happening inside the Cloud three approaches of gathering are established. Firstly all the relevant actions happening are directly sent to the EGM. These actions are enhanced with additional information such as the invoker of the action, the target as well as it's execution time. Not only basic-actions like file access or file removing are being gathered by the EGM but every higher level action as well. These actions refer to each other which enables forensic teams to reconstruct the whole situation. Additionally relevant, classified, log files are monitored and changes recorded in the EGM. This data is again matched to the corresponding action if available to better represent the situation. The last approach to gather data for the EGM are actions system information requests triggered by the EGM to gather meta data about the environment.

(ii) Metric matching: Metrics are defined to reflect legal aspects, access control regulations, SLA's and environment meta data. These metrics are matched against the data gathered by the EGM. If a match occurs the defined implication of the metric is gathered as meta data and included into the systems data. This step enhances the quality of the data gathered by the EGM and provides the possibility for automated security measures.

(iii) Data distribution: After each bit of gathered information, the EGM sends the data to all relevant listeners. To determine who is a relevant listener, potential destinations have to subscribe to the EGM providing a listener delegate. Through the meta data of the subscription the EGM know on which tier of the system the listener is located and whom it's relatives are. Every action is triggered with a target and an invoker, and depending on these properties the EGM sends the information of these action occurring to all listeners related to the invoker or the target. These data can be stored for later forensic investigations or can be parsed to activate a specific security measure.

IV. CONCLUSION

An event based evidence gathering mechanism is proposed to provide compliance with legal aspects regarding data protect as well as SLA regulations. Related frameworks lack the needed transparency through all layers of the cloud. Our planned research activities involve the development of example show case cloud application to derive CI requirements for cloud applications further. This will also include the involvement of stakeholders and experts in the legal domain to work on the legal aspects to event class mapping. This work will eventually help to set a security standard for audit-able logging information and therefore increase overall security and accountability of the cloud environment as well as enabling CI providers to outsource data handling into the Cloud.

REFERENCES

[1] F. Pallas et.al, "Seccrit public deliverable: Legal fundamentals (www.seccrit.eu)," 2013.

[2] R. Heames et al., "Data accountability in cloud using reliable log files forwarding," in *Int. Conf. on Inf. Comm. and Embedded Systems*, 2013.

[3] S. Chen, C. Wang, "Accountability as a service for the cloud," in *6th World Congress on Services*, 2010.

[4] A. Noman, C. Adams, "Data location assurance service for cloud comp. env." in *Tenth Annual Int. Conf. on Privacy, Security and Trust*, 2012.

[5] P. Massonet et al., "A monitoring and audit logging architecture for data location compliance in federated cloud inf." in *IEEE Int. Symposium on Parallel and Dist. Proc. Workshops and Phd Forum*, 2011.

[6] W. Wongthai et al., "A generic logging template for iaas cloud," in *27th Int. Conf. on Advanced Inf. Net. and Apps. Workshops*, 2013.

[7] S. Thorpe et al., "Cloud log forensics metadata analysis," in *IEEE 36th Int. Conf. on Comp. Software and Apps. Workshops*, 2012.

[8] R. Hunt, J. Slay, "The design of real-time adaptive forensically sound secure critical inf." in *4th Int. Conf. on N/W and Sys. Security*, 2010.