Towards Continuous Cloud Service Assurance for Critical Infrastructure IT

Aleksandar Hudic, Thomas Hecht, Markus Tauber
Austrian Institute of Technology
{alex.hudic, thomas.hecht, markus.tauber}@ait.ac.at

Andreas Mauthe
Lancaster University
a.mauthe@lancaster.ac.uk

Santiago Cáceres Elvira
ETRA Investigación y Desarrollo S.A.
scaceres.etra-id@grupoetra.com

***Abstract*—The momentum behind *Cloud Computing* has revolutionized how ICT services are provided, adopted and delivered. Features such as high scalability, fast provisioning, on demand resource availability makes it an attractive proposition for deploying complex and demanding systems. Clouds are also very suitable for deploying systems with unpredictable load patterns including *Critical infrastructure services*. Though, the major obstacle in hosting Critical infrastructures is often a lack of assurance. The transparency and flexibility offered by the Cloud, abstracts per definition over e.g. data placement, hardware, service migration. This makes it very hard to assure security properties. We present an investigation of assurance approaches, an analysis of their suitability for Critical Infrastructure Services being deployed in the Cloud and presents our approach.**

I. INTRODUCTION

Public utilities such as water, electricity, public transportation, health care system and telecommunication are vital assets of each society. Therefore, these assets are considered as the essential utility that drive economies and societies worldwide. Due to their crucial role, they are commonly referred in literature as Critical Infrastructure (CI) [1], [2], [3]. IT Systems used for managing CI require large resources, and hence CI providers often host their own infrastructure and possess own data centers.

A system defined by National Institute of Standards and Technology[1] (NIST), is a model for providing ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources, is more familiar under the term *Cloud Computing*. However, multitude of services offered by the Cloud makes it a viable proposition to embrace the Critical infrastructures in the Cloud environment (e.g. resilience to natural disasters, faster recovery in case of failure, redundancy, etc.), but it also results in new challenges as well (e.g. Loss of human-operated control for verifying security and privacy settings, week authentication and access control, denial of service, service failures, interference attacks, locality and legislative issues, data recovery issues, violation of service agreements, etc.). The very nature of cloud computing means that a service built on top of it comprises a multitude of heterogeneous components. The combination of these components may vary over time and administrative and/or geographical boundaries. This makes it hard to assure security properties of the deployed services – this is however of great importance of CI Systems.

We hence focus on investigating how existing assurance approaches can be applied to Cloud when being used for deploying CI services. Assurance in this context refers to guaranteeing security properties of a service which stores and process CI data inside the Cloud. A more detailed definition of assurance follows in the Section II.

This results into various research questions for assurance:

- How to derive a cloud service's overall assurance if individual assurance levels have to be aggregated?
- How to provide continuous assurance of a system?
- How to aggregate assurance levels across various legislative and administration boundaries?
- How to process assurance evaluation in an automated manner, and which guidelines exist?
- What are the issues related with Assurance for CI hosted in Cloud ecosystem?

In Section II we define assurance, outline our objectives, and illustrate the scope of our problem space. In Section III we show applied assurance as used within our research project. Section IV presents a comprehensive state-of-the-art evaluation and a discussion about shortcomings of exiting approaches in respect to our research questions and CI requirements. Finally we conclude the paper and present our future regarding the development of an assurance approach, for the given CI context, in section V.

II. ASSURANCE

Mechanism offered by each Cloud provider nowadays, for ensuring quality of service, are mainly based on Service Level Agreements (SLA). However, SLAs define mainly a predefined probability for delivering specific services in the Cloud environment. What is lacking in a SLA [4], is the assurance that measurable security & privacy properties & mechanisms are continuously met. For example, for data or information inside an ICT system, one of many challenges/requirements is a well-defined level of data confidentiality in order to maintain privacy across administrative and geographical borders. To ensure the data confidentiality the most easiest and intuitive approach would be to encrypt and to restrict the access. The user's data in order to reduce performance and processing costs is often stored unencrypted. The drawback of the approach, (i.e. leaving the data unprotected), is that it opens the possibility for significant data losses or exposures to unauthorized parties. Another example refers to deployment of virtual machines on the top of a Cloud's infrastructure layer, depending on the network and infrastructure components. Short outage of the only one component, regardless of the source of failure, regular firmware or software upgrades, migration on new virtualization stack, mitigates the possibility to continuously insure service

[1]NIST, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

978-1-4244-8396-9/10/$26.00

or information provisioning. In order to ensure that appropriate measures in the Cloud are met, we have to analyze and estimate each individual system components, services or actions.
Research directed towards this investigates if proper measures and actions have been undertaken to protect the data through its life cycle. This is known as Information Assurance. The USA's Department of Defense [5] defined information assurance as a measure that protects and defends information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
For the purpose of this paper the overall assurance is observed in respect to the proposed architecture and it's dynamic and volatile properties. Therefore, in respect with [5], we extend the ***assurance*** definition as the volatile property of a dynamic ICT system which enables to quantify each individual component based upon the confidence to reliably determine integrity, availability and confidentiality of the data or the services that the system provides. Furthermore, we additionally distinguish the following two assurance elements: ***System assurance*** and ***Information assurance***, defined as it follows:

- System assurance defines the assurance of individual components of a system such as service, class, or a module, and their mutual correlations.
- Information assurance defines the assurance of the data governance in respect to a single element or component.

In order to achieve the overall aggregation of all entities in respect with their dynamic properties, the above mentioned assurance elements are classified per the following three dimensions: standalone entities that are able to produce output based on the incoming input, *component*; set of individual components compounded to deliver a service, *layer*; and connections between the individual components which mutually deliver information or service, *dependency*. Finally, our goal is to ensure the continuity in delivering assurance regardless if we are taking in to consideration a single element, a layer or a whole system. Hence, we consider dynamic properties as a crucial element for delivering continuous assurance. For achieving the continuous assurance, we tend to investigate the how often and in which intervals should we evaluate particular assurance properties. We are motivated by the work [6] for investigating intervals and the work [7], [8], [9]

III. ASSURANCE AND SECCRIT: A CASE STUDY

A. SECCRIT architecture

We investigate our research questions and objectives within the scope of the SEcure Cloud computing for Critical infrastructure IT (SECCRIT) project. The SECCRIT project's mission is to identify relevant legal frameworks and establishment of respective guidelines, provisioning of evidence and data protection for cloud services; understanding, assessing and managing risk associated with cloud environments; establishing best practice for secure cloud service implementations; and the demonstration of SECCRIT research and development results in real-world application scenarios. An important contribution of SECCRIT is to provide a reference architecture [10], depicted in Figure 1, for supporting the development of technical solution for the provisioning of evidence and data protection for cloud services [11]. The level based classification addresses

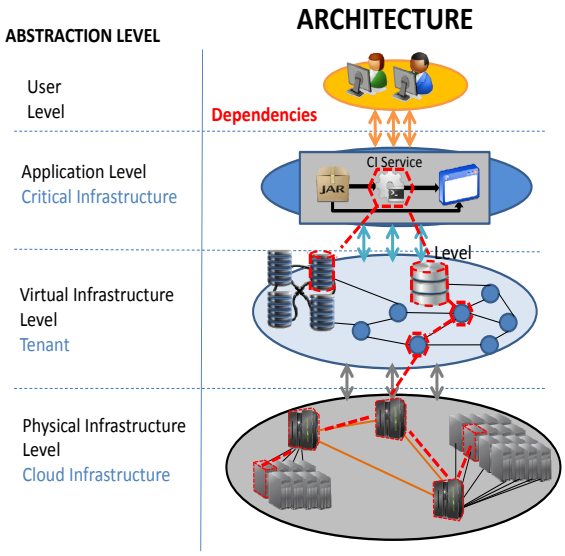

Fig. 1. Components and dependencies relevant for assuring application level security properties, illustrated in an architectural framework[10]. The left hand side of the figure depicts the abstraction levels of the architecture used for distinguishing individual assurance levels, which are additionally granulated through level components/elements.

directly the levels depicted on the left hand side of the Figure 1, and granularity is based on the individual components in particular level of the architecture.

B. Assurance in SECCRIT

The SECCRIT architecture, illustrated in Figure 1, is a structured approach for conducting our research on assurance for CI IT in the Cloud. Therefore, we also refer to the SECCRIT architecture[10] – which addresses the specific requirements of CI providers. Consequently within the scope of this work we propose a solution for addressing continuous assurance in Cloud ecosystem. The following set of properties & elements in line with the SECCRIT architecture, introduced in Figure 1, for assessing assurance should be considered:

- **Service components:**
  volatile elements: modules, classes and services;
  level: Application Level
- **Application components**
  volatile elements: API, frameworks, libraries;
  level: Application Level
- **Platform components**
  volatile elements: operating system, policies;
  level: Virtual Infrastructure Level
- **Virtual components**
  volatile elements: hypervisor, computational infrastructure components (server, network and storage:);
  level: Virtual Infrastructure Level
- **Physical network infrastructure components**
  volatile elements: network components, firmware updates, additional hardware features;
  level: Physical Infrastructure Level

We revise the SECCRIT architecture based on aforementioned properties in the following subsections, in respect to the three dimensions defined in Section II and dynamic properties of individual component.

1) Component Assurance Properties: The referred SECCRIT architectural model enables the fine-grained specification of privacy, security and resilience requirements, which are

upheld by the cloud infrastructure. Such objects should also considered when talking about assurance. We hence to use this model in order to illustrate its individual components,(i.e. marked red on Figure 1). A property change could imply a new assurance level for the individual component and also the entire cloud service. Therefore, we abstract these individual components first per the following abstraction levels: Application Level, Virtual Infrastructure Level and Physical Infrastructure Level. Afterwards, each individual component should be independently assessed. The next step is to aggregate individual assessments per an abstraction level, and finally to aggregate abstraction level in a bottom-up approach for providing a holistic assurance assessment.

2) Dynamic Assurance Properties: Dynamic parameters of individual components,(i.e. the volatile objects mentioned above) cause the deviation of assurance during time despite the component, level, observed system or assurance element. For example, in case of dynamic allocation of additional virtual components (volatile objects), the aggregated assurance level of the service provided had to be re-evaluated automatically in time. The end goal is always to merge the assurance to assess an entire cloud service with an aggregated assurance. Another potential use cease where under the consideration of a case in which a self-healing mechanism adds a new component to the infrastructure layer to support recovery from an attack, it is not sure that the new component has the same assurance level like the other ones. Hence a low assurance level might not have such a heavy impact on the tenant system or the overall assurance of the service provided.

3) Dependability in component based systems: The mutual interaction of individual system components on various level is a mandatory prerequisite for delivering overall service. In order to address assurance in such system, the dependability is considered as an important property of assurance that should be included in the assessment.

C. Assurance Evaluation criteria

To properly address the research objectives due to the above mentioned objects we conduct the evaluation of the state-of-the-art related towards assurance in the Cloud to the best of our knowledge. Hence for qualitative assessment we provide the following set of evaluation criteria:

1) Assurance in the Cloud
2) Geo-locality
3) Homogeneous system
4) Heterogeneous system
5) Static infrastructure assessment
6) Dynamic infrastructure assessment
7) Data/Information assurance
8) System/Service assurance
9) Flexibility towards the evaluated system
10) Continuous assurance
11) Information assurance Definition
12) Aggregation of assurance

These criteria set is derived in according to the research objectives, the property set for assessing assurance and the SECCRIT architecture, respectively. The prior concern was to evaluate the existing work related with assurance for hosting Critical infrastructures in Cloud environments. Then, we considered the scalability of services in Cloud over difference geographical boundaries. Next point that we address is the system architecture depending on how the analysis was approached (holistic view as a single entity or Granular view - component based). The follow-up to the previous point distinguishes how the components in the system are considered (Static or dynamic) and if they address the two assurance elements (Information and system) addressed in the extension of our assurance definition. Clearly we wanted also to see how the proposed work is flexible towards the type of the system being evaluated. One of the points included from the research questions were the capability of the system to aggregate the assurance and provide continuous assurance, respectively. Finally we wanted to see who provided the formal definition of the assurance.

IV. STATE OF THE ART EVALUATION

We summarize, to the best of our knowledge, existing guidelines, methodologies, standards and approaches of closely related projects in respect to Assurance of Critical infrastructures hosted on top of the Cloud ecosystem. In particular, we investigate how the existing approaches confront the challenges and our research objectives mentioned in the previous section.

A. Guidelines

1) IT assurance Guide by COBIT: The goal of COBIT's IT Assurance Guideline [12] is to support and guide enterprises to leverage COBIT framework for variety of IT assurance activities. The guide is designed to support efficient and effective development of IT assurance initiatives, providing guidance on planning, scoping and executing assurance reviews using a road map based on well-accepted assurance approaches. The IT Assurance Guide provides assurance advice at the process and the control objective level. Furthermore, the guideline also implements the assessment processes in respect with the business plan, through the following three stages: planning, scoping and executing. First phase defines the universe of the assurance (the observed entities), selects an IT control framework, defines the set of preferred objectives, performs high level assessment and risk assurance planning. The second phase, defines in respect with the business model IT goals and key processes, resources and custom control objectives. The final phase refines the understanding of IT assurance subject and the scope of key control objectives, tests effectiveness and outcome of the key control objectives, setups the final conclusion and documents the impact on control weaknesses. COBIT guideline offers a fine grained analysis of the system with in respect to business goals, however it leaks the support for critical infrastructure and assurance in respect to Cloud ecosystems, locality issues, and aggregation of assurance.

2) Information Technology Assurance Framework: Information Technology Assurance Framework (ITAF) [13] is a comprehensive best practice guideline that provides design, guidance, implementation and reporting of IT audits and assurance assignments, defines concepts and terminologies in respect to IT assurance, and establishes set of reporting and auditing requirements. ITAF is composed of three standard guidelines: General set of standards, Performance Standards and Reporting Standards. The framework also operates and addresses other guidelines such as COBIT, ITIL, (ISO)/IEC 27000 standards, IT Control Objectives, IT Governance Domain Practices and Competencies, within the scope of his work to assess the IT infrastructure.

The framework is a adhering the above mentioned standards as a set of relevant requirements of an IT professional dealing with this IT assurance, and more tending towards guideline

for best practices for business and IT processes, in respect of assurance and audit standards. Therefore, making it a well structured, comprehensive and eligible best practice for IT business processes evaluation.
The ITAF derives best practices and strategic approaches to provide holistic assurance of a system, however doesn't address neither the critical or cloud infrastructures.

3) Cloud Computing Information Assurance Framework: ENISA's Information Assurance Framework [14] derives set of assurance criteria for: assessment of the risk for adopting cloud technologies, comparing various distinct cloud offerings, business and management process analysis and system policies. The framework is interesting only in terms of risk analysis for adopting cloud services, in our case this would be adopting critical infrastructure services, otherwise it cannot support more comprehensive analysis that we require.

4) National Security Agency Information Assurance Directorate: National Security Agency Information Assurance Directorate [15] provides an exhaustive assessment of the maturity and suitability of relevant IA technologies for meeting information assurance required capabilities. The directorate highlights four main cornerstones: Assured Information Sharing, Highly Available Enterprise, Assured Enterprise Management and Control and Cyber Situational Awareness and Network Defense. The cornerstones are mapped to Information Assurance System Enablers (Identification & Authentication, Policy Based Access Control, Protection of User Information, Dynamic Policy Management, Assured Resource Allocation, Network Defense & Situational Awareness and Management of IA Mechanisms & Assets) for a more convenient analysis and organization. The IA directorate advocates methodologies and best practices that should be conducted in order to achieve the assurance IA Components. Fine granulation is achieved through components and system enablers what are wrapped up with Information Assurance cornerstones. IA system enablers are mapped to sets of technology categories and mechanism, therefore regardless of the ability to wide and comprehensive application, the directorate is still repelling to changes.
Information Assurance Directorate addresses the problem of critical infrastructures in the scope of his work, but unfortunately without concerning the issues (e.g. locality issues which are also covered with our evaluation) relevant to hosting it on top of cloud infrastructures.

5) Handbook for Information Assurance Security Policy: This Handbook [16] is used to derive information assurance security policies complied with federal laws and regulations. The primary focus of this document are policies and guidelines that supports the IA Security Program in protecting the confidentiality, integrity, and availability of the Departments systems and information life cycle. Additionally, the handbook is reinforced through a series of standards, directives, and other procedures documents that address specific aspects of the IA Security Policy.
The handbook advocates set of management, operational and technical controls that undergo the referenced various guidelines and standards from the Office of Management and Budget, National Institute of Standards and Technology, General Services Administration and the Office of Personnel Management. Therefore it doesn't meet our objectives for supporting dynamic and flexible systems, continuous assurance, critical infrastructures in cloud environments or geo-locality issues in distributed environments.

6) Department of Defense Directives 8500.01 and 8500.02: Information assurance integrated in Department of Defense (DoD) Directives 8500.01 and 8500.02 [17], [18] derive a set of requirements that should be identified and included in the design, acquisition, installation, upgrade, or replacement of any information system within DoD. Whereby directive is pointer towards maintaining an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability. Directive efficiently utilizes defense-in-depth approach that integrates the capabilities of personnel, operations, and technology.
Both directives were built upon DoD's ICT systems, and therefore address information assurance concerns that are only related to DoD's systems, which makes them less applicable and limiting for broader usage.

7) Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy : This document [5] derives strategies to organize for unity of purpose and speed of actions, enable secure mission-driven access to information and services, anticipate and prevent successful attacks on data and networks, and prepare for and operate through cyber degradation or attack. The focus of this work is to establish a narrow-down set of strategic activities for maintaining and insuring information assurance, which unfortunately covers only a minor part of our objectives regarding assurance.

8) Information Assurance Governance Framework: The Information Assurance Governance Framework [19] is focused to derive functional and managerial hierarchy for information assurance, risk management procedures and guidelines, and to identify mechanisms, procedures and best practices for facilitating information assurance. The main focus of the framework is pointed on facilitating management and risk confidence of the stakeholders. Therefore, this framework is oriented on business aspects rather then technical which we are addressing as the priority of our work.

9) Common Criteria: The Common Criteria for Information Technology Security Evaluation framework[2] [20] is a well-known approach to apply rigorous engineering methods and processes to the design and development of security and critical IT systems. Common Criteria (CC) provide the process of specification, implementation, and evaluation of security-critical, high-assurance systems in a rigorous and standardized manner. The key concept of CC is that by testing a security product against defined security properties of the product, it can be determined with high confidence if the product can actually meet its claims. In a CC evaluation process, a Target Of Evaluation (TOE) is the product or system under evaluation. A user or a user community identifies common security requirements on a class of devices or systems such as access control devices and systems or key management systems in the Protection Profile (PP) document. A Security Target (ST) document contains the IT security requirements of the TOE and specifies the functional and assurance measures offered by the TOE to meet these requirements. The effort of the evaluation process is ranked numerically from one to seven in Evaluation Assurance Levels (EAL). CC provides not only a benchmark for security "'due diligence"' checking, but also assurance on the design, development, deployment, and life-cycle handling of security-critical systems. CC can significantly increase the security of a software/hardware system

[2]Common Criteria, http://www.commoncriteriaportal.org/

as well as the confidence of the end-user of the system by emphasizing good and comprehensive documentation during the system design and development phase. At this the system development team has security as its main objective from the very beginning. There is also a raise of awareness related with security problems throughout the system's design and development phases.
Regardless of the rich set of features facilitated by the framework, it still doesn't support the aggregation of different assurance levels for individual components, concerns the systems hosted in Cloud, or derive a continuous assurance. Therefore this has to be resolved in order to overcome the problems mentioned in the introduction section of this paper. However, the approach of Common Criteria offers a solid foundation for building components based assurance framework for critical infrastructures in the Cloud ecosystem.

10)Cloud Trust Protocol: The Cloud Trust Protocol (CTP) is the mechanism which offers cloud users to request and acquire information about the elements of transparency as applied to cloud service providers. The primary purpose of the CTP and the elements of transparency is to generate evidence-based confidence that everything that is claimed to be happening in the cloud is indeed happening as described. This is a classic application of the definition of digital trust. And, assured of such evidence, cloud consumers become liberated to bring more sensitive and valuable business functions to the cloud, and reap even larger pay-offs. With the CTP cloud consumers are provided a way to find out important pieces of information concerning the compliance, security, privacy, integrity, and operational security history of service elements being performed "in the cloud".
These important pieces of information are known as the "elements of transparency", and they deliver evidence about essential security configuration and operational characteristics for systems deployed in the cloud. The elements of transparency empower the cloud consumer with the right information to make the right choices about what processing and data to put in the cloud or leave in the cloud, and to decide which cloud is best suited to satisfy processing needs. This is the nature of digital trust, and reinforces again why such reclaimed transparency is so essential to new enterprise value creation. Information transparency is at the root of digital trust, and thus the source of value capture and pay-off. [21]
Cloud Trust Protocol facilitates data acquisition over distinct cloud providers is a large benefit towards achieving transparency but unfortunately it doesn't assurance of the actions been really conducted from the provider (for example location of the data, how can we know that some part or the whole data set hasn't been replicated on some other location).

B. Projects

1) Cumulus: CUMULUS is aligned with the recommendations of a recent industrial consultation to the European Commission which identified cloud certification as an enabling technology for building trust for end users through the deployment of standards and certification schemes relevant to cloud solutions, and included it in the ten key recommendations and actions for a cloud strategy in Europe [22].The project develops an integrated framework of models, processes and tools supporting the certification of security properties of infrastructure (IaaS), platform (PaaS) and software application layer (SaaS) services in cloud. The framework will bring service users, service providers and cloud suppliers to work together with certification authorities in order to ensure security certificate validity in the ever-changing cloud environment. The project relies on multiple types of evidence regarding security, including service testing and monitoring data and trusted computing proofs, and based on models for hybrid, incremental and multi-layer security certification. To ensure large-scale industrial applicability, this framework will be evaluated in reference to cloud application scenarios in some key industrial domains, namely smart cities and eHealth services and applications. Therefore, the certification model is an attractive solution for handling security parameters that have to be meet inside of a system. However, at the moment the approach addresses only single level certification within his scope without the aggregation of the levels, but it addresses the same core problem of meeting security requirements.

2) A4Cloud: The Cloud Accountability Project (or A4Cloud for short) focuses on the accountability for cloud and other future internet services as the most critical prerequisite for effective governance and control of corporate and private data processed by cloud-based IT services. The research being conducted in the project will increase trust in cloud computing by devising methods and tools, through which cloud stakeholders can be made accountable for the privacy and confidentiality of information held in the cloud. These methods and tools will combine risk analysis, policy enforcement, monitoring and compliance auditing. They will contribute to the governance of cloud activities, providing transparency and assisting legal, regulatory and socio-economic policy enforcement. [23]In [24], [25], as a part of the A4Cloud project, authors comprehensively address accountability pointed towards governance.
A4Cloud project addresses assurance indirectly under the scope of accountability within respect to the data governance. The comprehensive approach conducted to ensure the accountability correlates with our scope and goals, the difference that we base our work on hosting critical infrastructures on top of cloud stack.

3) MYSEA: The Monterey Security Architecture [26](MYSEA)[3] is a research project to build a robust enterprise-level architecture that provides multi-domain authentication and security policy enforcement. The MYSEA cloud consists of high-assurance servers and authentication components for security services. The high assurance of MYSEA cloud is built on a trusted server (i.e., an EAL5-augmented trusted platform) and authentication component (i.e., an EAL7 Least Privilege Separation Kernel). Originally aiming at composing secure distributed systems using commercial off-the-shelf components, some of the results from the MYSEA project might also be applicable to cloud computing environment.
Regarding the topic of our paper, MYSEA only consists of a few components evaluated with a certain assurance level (trusted server and authentication component). There is no necessity of aggregating different assurance levels of different components. An advantage of this architecture is, that clients, respectively cloud service users, also are considered due to security reasons. In the case of a given assurance level framework, there is the gap of what is the right treatment of

[3]Monterey Security Architecture (MYSEA), Centres for Information Systems Security Studies and Research at Naval Postgraduate School, U.S., http://www.cisr.us/projects/mysea.html

an unprotected cloud service user which wants to connect to the service.

C. Discussion

We carried out a comprehensive state-of-the-art evaluation approaches, methodologies, procedures, guidelines and projects related with system and information assurance of critical infrastructures hosted on top of Cloud ecosystems. The Cloud ecosystems, as anticipated, can offer full support to internet scale critical applications (e.g. hospital systems and smart grid systems). Unfortunately, organizations refuse to outsource their resources, regardless if critical or not, without confidence that a proper set of actions and measures are undertaken to provide information and system assurance. The approaches such as mentioned in the work [27] support scalable critical applications over the Cloud infrastructure, by providing assurance to cloud users related with the trustworthiness of service delivery in a cloud environments, known as operational trust. Particular focus is on analyzing the most important properties (adaptability, scalability, resilience, availability and reliability) within a cloud, which enable assessments of the operational trustworthiness or effectiveness of a cloud provider for delivering these services. The assessment of operational trust enables cloud service users, auditors, collaborating cloud providers, and others to improve the decision making and quantifying cloud providers. Additionally in [28] authors advise a trust-overlay network over multiple data centers to implement a reputation system for establishing trust between service providers and data owners. In order to offer additional layer of security and trustworthiness data coloring and software watermarking techniques protect shared data objects and massively distributed software modules. These techniques safeguard multi-way authentication, enable single sign-on in the cloud, and tighten access control for sensitive data in both public and private clouds.

The outcome of our comprehensive state-of-the-art evaluation is presented in Table I that can be found on page 7. We classify two venues for our inquisition: Frameworks/Guidelines/Standards/Policies and assurance related Projects.

Primarily, we focused on inquiring and evaluating the work that covers the domain issues related with Critical infrastructures and Assurance. Although critical infrastructures are a specific and broad domain, additionally hosting them on top of Cloud infrastructure extends their perimeter and improves the performance, However also it raises new challenges related to security, privacy, availability, verifiability, etc. that we observer under the term of assurance. The National Security Agency (NSA) in the Information Assurance Directorate [15] and Department of Education (DoE) in the Handbook for Information Assurance Security Policy [16] reference in scope of their work general assurance requirements related with critical infrastructures. One of our main points of interest also related with the work done as a part of SECCRIT project is to investigate locality challenges and issues, therefore we include geo-locality concerns (e.g. legislative issues confronted by cross administrative and regional migrations). Geo-locality has been addressed by several large organizations, such as National Security Agency, ENISA, Department of Defense, Department of Education, and A4Cloud research project. The [14], [16], [18], [20], [21], [23], [26] referred to the geo-locality as as an obligatory part of a federal or local law, whereby in our case we would like to consider it as cross domain (geographical, federal, regional, administrative) issue required for assessing overall assurance. Next to our interest is the observation perspective of a system, where we wanted to investigate if the system was observed from a holistic or a homogeneous perspective. Majority of the work that was evaluated [12], [13], [14], [15], [16], [17], [18], [5], [26], [23], [22], [20], [26] derived their work in a holistic manner, with minority of approaches [14], [20], [23], [22], [26] that focused to observe system in a heterogeneous manner. Furthermore we wanted to see how does a particular state-of-the-art work observe the properties of a system over time. Therefore, we focused to evaluate if state-of-the-art work is capable of confronting dynamic system changes such as component, class, modules, vendor, etc. that can change their functionalities and characteristics. In particular, the work of [12], [13], [14], [15], [16], [5], [20], [23], [22] refers to a static system observation, whereby the work of [20], [12], [23], [22] due to their flexibility in the approaches are able to granulate system through components and deal with dynamic changes of a system. The next point of our evaluation is observed within respect to the definition of assurance and it's elements (data and service assurance). The majority of the evaluated state-of-the-art-work [12], [14], [15], [16], [17], [18], [5], [19], [20], [23], [26] derived the work in both system and information assurance, whereby the remaining work [13], [21], [22] didn't address this issue at all. Despite the fact that CUMULUS [22] doesn't directly address the assurance, the major benefit of their approach is the ability to continuously deliver assurance through the certificates that they deliver only per individual level. Furthermore we wanted to see who defines the assurance to avoid ambiguity of term being used in general manner. Unfortunately, only minor part of the evaluated work [13], [17], [18], [5], [19], [20], [23] formalized the assurance in form of a definition within respect of particular objectives. As the last point of our evaluation we inquire the capability of the state-of-the-art approaches to aggregate the assurance of individual components for evaluating a system as a whole. Only the approaches [20], [21], [23], [22] have addressed the problem of information aggregation to holistically observe some system.

V. CONCLUSION AND FUTURE WORK

We have identified a number of issues regarding assurance of CI in the cloud and identified short-comes via a comprehensive evaluation of existing approaches. As a result we propose as a part of the conclusion a new assurance approach and framework as the basis of our future work.

A. Conclusion

This work identified the set of problems, stated as research questions (Section 1),which address assurance for those systems that require specific care when hosting in Cloud environments (i.e. Critical infrastructures). Furthermore, we investigated the shortcomings of existing methodologies, guidelines, frameworks, standards and projects for supporting high assurance in Cloud environments and SECCRIT architecture, respectively. Our evaluation outcomes that the current work in Cloud environments lacks clarity and executability for identifying security requirements and security properties of higher-assurance systems for critical infrastructures in cloud computing. Considering our research objectives, the main drawback of the methodologies, guidelines, frameworks and standards for assessing assurance in cloud is the support for

TABLE I. EVALUATION OF THE STATE OF THE ART APPROACHES FOR ADDRESSING ASSURANCE IN CLOUD ECOSYSTEMS

	Frameworks/Guidelines/Standards										Projects		
	IT Assurance Guide	Information Technology Assurance Framework	Cloud Computing Information Assurance Framework	Information Assurance Directorate	Handbook for Information Assurance Security Policy	Directives 8500.01 and 8500.02	Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy	Information Assurance Governance Framework	Common Criteria for Information Technology Security Evaluation Framework	Cloud Trust Protocol	Certification infrastructure for multi-layer cloud services project	A4Cloud project	The Monterey Security Architecture
Assurance in the Cloud				✓	✓								✓
Geo-locality			✓		✓	✓			✓	✓		✓	
Homogen system	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓
Heterogeneous system			✓						✓		✓	✓	✓
Static infrastructure assessment	✓	✓	✓	✓	✓		✓		✓		✓	✓	✓
Dynamic infrastructure assessment	✓								✓		✓	✓	
Data/Information assurance	✓		✓	✓	✓	✓	✓	✓	✓			✓	✓
System/Service assurance	✓		✓	✓	✓	✓	✓	✓	✓			✓	✓
Continuous assurance											✓		
Information assurance Definition		✓				✓	✓	✓	✓			✓	
Aggregation of assurance									✓	✓	✓	✓	

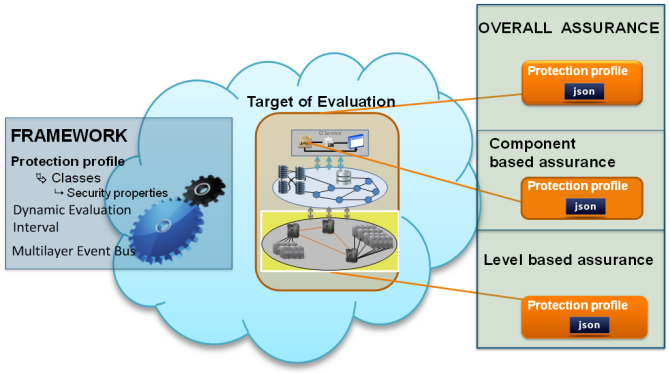

Fig. 2. Our Assurance Assessment Framework for assessing CI services hosted in the Cloud. The framework is based on classes (i.e. confidentiality, availability, etc.) which are motivated by Common Criteria [20] protection profiles. Protection profiles will be derived for the whole system, for each abstraction level and individual component. This is based on existing work [6], [29]

hosting CI in the Cloud. The evaluation showed that only the concepts used in the work of Common Criteria, CUMULUS and A4Cloud are partially eligible to resolve the challenges for hosting CI in the cloud. Whereby, Common Criteria allows us to evaluate traditional IT component based system, dependencies of components, comparability between the results of independent security evaluations and overlaps with the security consideration of our assurance definition. However, additional extensions of the framework are required to completely support our research objectives like aggregation of assurance, continuous assurance or automated assurance within respect Cloud ecosystem. CUMULUS project delivers the important feature certification of continuous monitoring [30] that we can adopt to support continuous assurance. A4Cloud addresses the issue of assurance in the cloud under the term of accountability and corporate data governance, which also doesn't completely fulfill our requirements.

Despite that there are approaches derived for addressing assurance, mostly addressing information assurance, the evaluation showed that a framework for extensive analysis of assurance in Cloud ecosystem is required. Therefore, an independent framework for addressing assurance in Cloud-based systems would require to address the following: assurance of the systems hosted on top of the Cloud, delivering assurance continuously at any point of time; classifying assurance per abstraction levels and components, based on the propose architecture; technology independent assessment; aggregating of assurance in automated manner.

Motivated by the outcome of our evaluation which clearly outlined the shortcomings of existing approaches for supporting the assurance in Cloud ecosystems and lack of any kind of solutions that would support it, we propose an independent *Assurance Assessment Framework* for assessing Critical infrastructures hosted on the top of the Cloud ecosystems, Figure 2. The proposed Assurance Assessment Framework, founded on our extended assurance definition, distinguishes the assurance in the system prior to the assurance elements (system assurance or information assurance). Each individual assurance element is additionally classified per component, layer or component dependency. For the purpose of the SECCRIT project we outlined dynamic properties per abstraction levels (user, application, virtual and physical infrastructure). Our Framework defines the Protection profile [20] in respect with dynamic properties of a component, layer or dependency, dynamic assessment interval [6] and Multilayer Event Bus [29]. Protection profile is composed of Classes (i.e. availability, confidentiality, integrity, etc.) where each individual class is depicted by a set of security properties. This framework configuration allows us to deliver customized assurance assessment per individual

component that can aggregated the assurance per abstraction levels, and finally overall assurance.

B. Future Work

The Assurance Assessment Framework was founded on the work delivered within the scope of SECCRIT project deliverables (D2.1[4],D2.2[5], D3.1[6] and D5.1[7]), that derived requirements of the use case scenarios, vulnerability catalogue, APIs for information acquiring, and auditing processes. Our future goal is to build our Assessment Framework for delivering continuous assurance by extend the well-known concepts of Common Criteria class based approach [20] to aggregate assurance in continuous manner, and the concepts of CUMULUS certification of continuous monitoring module [30].
For the empirical evaluation we will focus to build a proof of concept for acquiring information/evidence based on work [29], [7], [8], [9], per abstraction levels. To overcome the fallback of restricted information acquisition per level in case of different stakeholders and consider the work of [31], [32], [33], [34], [35] regarding privacy and security related concerns, as an alternative we will integrate and rely on the services offered by the Cloud provider (i.e. SLA, monitoring services or trust protocols).

ACKNOWLEDGMENT

This work has been funded from the European Unions Seventh Framework Programme for research as the SECCRIT project under grant agreement no 312758.

REFERENCES

[1] C. C. John Moteff, S. John Fischer Resources, and I. Division, "Critical infrastructures: What makes an infrastructure critical?" Congressional Research Service The Library of Congress 101 Independence Ave. SE Washington, DC 20540, Report for Congress, 2003.

[2] J. Moteff, C. Copeland, and J. Fischer, "Critical infrastructures: What makes an infrastructure critical?" DTIC Document, 2003.

[3] W. Krger, "Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools," *Reliability Engineering & System Safety*, vol. 93, no. 12, p. 17811787, 2008.

[4] L. Wu and R. Buyya, "Service level agreement (sla) in utility computing systems," *CoRR*, vol. abs/1010.2881, 2010.

[5] D. of Defense, *Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy*, 1st ed., Department of Defense, August 2009. [Online]. Available: http://dodcio.defense.gov

[6] M. Tauber, G. N. C. Kirby, and A. Dearle, "Autonomic management of maintenance scheduling in chord," *CoRR*, vol. abs/1006.1578, 2010.

[7] K. Mahbub, G. Spanoudakis, and T. Tsigkritis, "Translation of slas into monitoring specifications," in *Service Level Agreements for Cloud Computing*, P. Wieder, J. M. Butler, W. Theilmann, and R. Yahyapour, Eds. Springer New York, 2011.

[8] G. Spanoudakis, C. Kloukinas, and K. Mahbub, "The serenity runtime monitoring framework," in *Security and Dependability for Ambient Intelligence*, ser. Advances in Information Security, S. Kokolakis, A. M. Gmez, and G. Spanoudakis, Eds. Springer US, 2009, vol. 45.

[9] H. Foster and G. Spanoudakis, "Advanced service monitoring configurations with sla decomposition and selection," in *Proceedings of the 2011 ACM Symposium on Applied Computing*, ser. SAC '11. New York, NY, USA: ACM, 2011.

[4]Deliverable 2.1 - Report on requirements and use cases, https://www.seccrit.eu/upload/D2-1-Report_on_requirements_and_use_cases-v2.0

[5]Deliverable 2.2 - Legal fundamentals, https://www.seccrit.eu/upload/D2-2-Legal-Guidance-v2.0

[6]Deliverable 3.1 - Methodology for Risk Assessment and Management, https://www.seccrit.eu/upload/D3-1-Methodology-for-Risk-Assessment-and-Management

[7]Deliverable 5.1 - Design and API for Audit Trails and Root-Cause Analysis, https://www.seccrit.eu/upload/D5.1-Audit-Trails

[10] F. P. J. H. P. S. Marcus Schoeller, Roland Bless, "An architectural model for deploying critical infrastructure services in the cloud," *IEEE CloudCom 2013*, 2013.

[11] R. Bless, M. Flittner, J. Horneber, D. Hutchison, C. Jung, F. Pallas, M. Schller, S. N. H. ul Shirazi, S. Simpson, and P. Smith, "Whitepaper "af 1.0" seccrit architectural framework," 2014.

[12] COBIT, *IT Assurance Guide: Using COBIT*, Control Objectives for Information and related Technology, 2007, information Systems Audit and Control Association.

[13] ITAF, *Information Technology Assurance Framework*, 2nd ed., Information Systems Audit and Control Association, 2013.

[14] ENISA, *Cloud Computing Information Assurance Framework*, 1st ed., European Union Agency for Network and Information Security, 2009. [Online]. Available: http://www.enisa.europa.eu/

[15] NSA, *Information Assurance Directorate*, 1st ed., National Security Agency, 2010.

[16] D. of Education, *Handbook for Information Assurance Security Policy*, 1st ed., U.S. Department of Educations, 2005. [Online]. Available: http://www2.ed.gov/fund/contract/about/acs/acshbocio01.doc

[17] DoD, *Directives 8500.01*, 2nd ed., Department of Defense, May 2005. [Online]. Available: www.prim.osd.mil/Documents

[18] ——, *Directives 8500.02*, 1st ed., Department of Defense, 2003. [Online]. Available: www.prim.osd.mil/Documents

[19] CSIA, *Information Assurance Governance Framework*, 1st ed., CSIA, 2004. [Online]. Available: www.cabinetoffice.gov.uk

[20] CC, *Common Criteria for Information Technology Security Evaluation*, CCDB USB Working Group, 2012, part 1-3. [Online]. Available: http://www.commoncriteriaportal.org

[21] CSA, "Introduction to cloudtrust protocol," 2011. [Online]. Available: https://cloudsecurityalliance.org/research/ctp/

[22] CUMULUS, "Certification infrastructure for multi-layer cloud services project (cumulus)," 2012. [Online]. Available: http://www.cumulus-project.eu/index.php/description

[23] A4Cloud, "Cloud accountability project (a4cloud)," 2013. [Online]. Available: http://www.a4cloud.eu/

[24] M. Felici, T. Koulouris, and S. Pearson, "Accountability for data governance in cloud ecosystems."

[25] S. Pearson, "Toward accountability in the cloud." *IEEE Internet Computing*, vol. 15, no. 4, 2011.

[26] C. E. Irvine, T. D. Nguyen, D. J. Shifflett, T. E. Levin, J. Khosalim, C. Prince, P. C. Clark, and M. Gondree, "Mysea: The monterey security architecture," p. 3948, 2009.

[27] I. M. Abbadi, "Operational Trust in Cloud's Environment," *IEEE Symposium on Computers and Communications,*, p. 141145, 2011.

[28] D. L. Kai Hwang, "Trusted Cloud Computing with Secure Resources and Data Coloring," *IEEE Internet Computing*, vol. 14, Sept. 2010.

[29] M. Florian, S. Paudel, and M. Tauber, "Trustworthy evidence gathering mechanism for multilayer cloud compliance," in *ICITST*, 2013.

[30] M. Krotsiani, G. Spanoudakis, and K. Mahbub, "Incremental certification of cloud services," in *SECURWARE 2013, The Seventh International Conference on Emerging Security Information, Systems and Technologies*, 2013, p. 7280.

[31] Z. Fadlullah, T. Taleb, A. Vasilakos, M. Guizani, and N. Kato, "DTRAB: Combating Against Attacks on Encrypted Protocols Through Traffic-Feature Analysis," *IEEE/ACM Transactions on Networking*, 2010.

[32] L. Wei, H. Zhu, Z. Cao, W. Jia, and A. Vasilakos, "SecCloud: Bridging Secure Storage and Computation in Cloud," in *Distributed Computing Systems Workshops (ICDCSW)*, June 2010, p. 5261.

[33] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos, "Security and Privacy for Storage and Computation in Cloud Computing," *Inf. Sci.*, vol. 258, p. 371386, Feb. 2014.

[34] B. Liu, J. Bi, and A. Vasilakos, "Toward incentivizing anti-spoofing deployment," *Information Forensics and Security, IEEE Transactions on*, vol. 9, no. 3, p. 436450, March 2014.

[35] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile Cloud Computing: A Survey," *Future Gener. Comput. Syst.*, vol. 29, 2013.