Trust and Regulation Conceptualisation: The Foundation for User-Defined Cloud Policies

Jörg Kebbedies, Felix Kluge, Iris Braun, Alexander Schill

Trust and Regulation Conceptualisation: The Foundation for User-defined Cloud Policies

Jörg Kebbedies[1], Felix Kluge[2], Iris Braun, and Alexander Schill

[1] Technische Universität Dresden, Faculty of Computer Science, 01062 Dresden, Germany,
joerg.kebbedies@mailbox.tu-dresden.de,
[2] Technische Universität Dresden, Faculty of Computer Science, 01062 Dresden, Germany

Abstract. In the areas of secrecy or sensitive data management, the public cloud paradigm is not currently well accepted. The root of this problem arises from an inherent structural concept of restricted responsibilities and the lack of trust from the cloud users' perspective.
This work introduces a conceptual approach to user-centric policy management for cloud usage, combined with an underpinning holistic trust approach. Trust has to be established as a separate infrastructural concept determining the level of user adjustability. This approach outlines how provisioning cloud users' policies is combined with agent-based trust establishment. An ontology-driven regulation concept enables formal policy definitions and trustworthy real-time reasoning about current trust levels, policy states, and pending security risks.

Keywords: trust, cloud, regulation, policy, ontology, logic-based semantic

1 Introduction

Although the proliferation of cloud computing seems to gradually be gaining social recognition, the public cloud sector still lacks well-defined user acceptance in specific business areas with high secrecy and privacy requirements. In the past, this issue was discussed in detail in different studies from BITKOM [2] and BSI [4], which have proved that a lack of trust and fear of risk in public cloud services is the main obstacle to common user acceptance.

Trust becomes the fundamental key approach to open the public cloud for use cases with high demands for security and privacy. Once the importance of trust is established, a new problem arises from its nature. The level to which we can be confident that a prescribed security policy controls a given behaviour is the point that defines the level of trust assurance in general. The level at which one can be confident that a behaviour is confined within a prescribed security policy defines the level of trust assurance [3, Page 28] but trust can only be justified through future confidence.

One of the biggest challenges is developing well-suited cloud user control instruments to ascertain the accuracy of ones trust. Following the strategy of trust

enables coupled organisations to gradually stabilise their relationship properties. The new dimensions resulting from trust–confidence in measured properties rather than blind trust–will have an important impact on cloud computing.

In this paper, we propose one instrument to formalise trust.

2 The Principles of Expectation in a Cloud Context

Adapting social principles of expectation to the cloud requires a full understanding of the concepts *Semantic*, *Receipt*, *Success* to develop coordinating and expected pattern of behaviours. The user may define their expectations in terms of policies, role definitions, or regulations for security, privacy, and reliability, but the fact remains that all intended goals are not predictable and this reduces the likelihood that public cloud usage will be accepted in regulated markets.

It is essential to build semantically richer representations of regulations (*Semantic*). An unmistakable interpretation is one of the main factors in achieving reliable technical transformations. The process of defining policies needs formal linguistic instruments to express regulations; these regulations must be independent of specific business domains but should stay readable for people in regard to different legal-requirement categories [17],[1],[8].

The aspect of *Receipt* is strongly involved with trustworthy technical entities. Trustworthy and evaluated cloud entities, acting on behalf of the cloud user, are the foundations of the cloud user's confidence and extend his policy management scope. Such entities, which are introduced in Sec. 3.1, are technically realised through knowledge-driven cloud agents, able to enforce a cloud user's policies in a reliable and trustworthy manner [11].

The aspect of *Success* can only be guaranteed through a strong link between the cloud user's policy definitions and the trustworthy policy-enforcing entities. Only a measurable concept of trust successfully establishes the cloud user's confidence that his regulation requirements will be reliably enforced and remain compliant in regard to his expectations.

3 The Trust Concept

Following the arguments from Sec. 2, the strong relationship between regulation and trust can be emphasised. Unfortunately, current standardisation efforts like TOSCA [12] to provide flexible and efficient capabilities for service orchestration, service deployment, and cloud-application policy management follow a functionally driven approach; they do not currently provide bases of trust commensurate with their objectives to improve life-cycle processes for cloud-service provisioning and policy management.

Above all other security aspects, the central key concept is a trusted identity. The assurance in identity established by secure authentication is a necessary condition of regulation. Once users securely authenticate an entity based on its claimed identity, a security context has to be established to regulate its states and behaviour.

3.1 Trustworthy Knowledge-based Agent

The architectural design depicted in Fig. 1 outlines the main process of enforcing different conceptualised policies in a public cloud architecture.

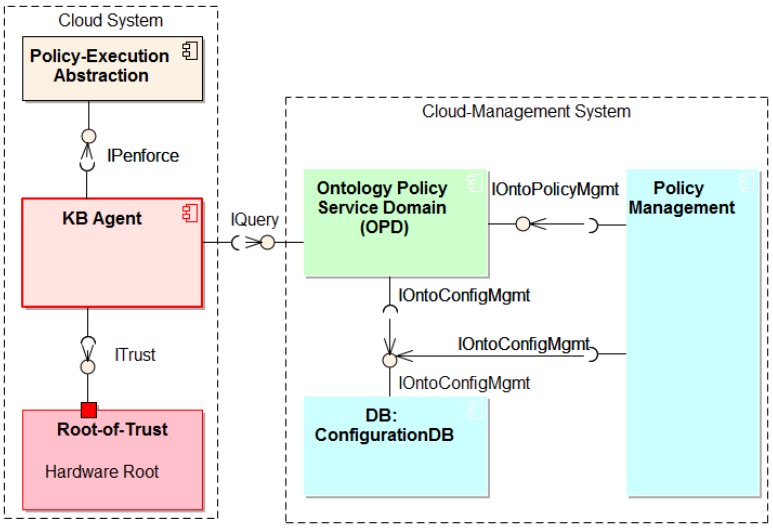

Fig. 1. Knowledge-based agent architecture

The knowledge-based agent (KB Agent) demonstrates that a scope of regulation can only be successfully extended if the transition follows a prepared chain of points of trust. For that reason, each agent has to be technically linked to a root-of-trust (see interface *ITrust*) using the Trust-Establishment-Protocol introduced in Sec. 3.3.

The knowledge-based agent is connected to a knowledge base using the interface *IQuery*, which is represented through a multiple ontology providing formal described regulation instructions. Based on the interface *IPenforce*, the knowledge-based agent is responsible for realising a concept of *Transformation* formally defined in the regulation ontology.

The *Transformation* concept is a bridge between a knowledge-based modelled policy concept and a concrete external cloud system. The subconcepts of Transformation are responsible for adapting declarative defined rules into system-specific, technically executable instructions.

Within the prior work [11], different technical approaches were evaluated and some were implemented as part of a proof of concept. The component *Policy-Execution Abstraction* depicted in Fig. 1 represents a Java-based realisation of Transformation.

3.2 Trust-Hierarchy Provisioning

Regulations have to find a base of trust as a precondition to effectively acting on the cloud user's intentions. The topic of trust becomes an ingrained part of the concept of regulation, expressing their intrinsic value as a whole.

The model of a Knowledge-based-Agent (KB Agent) approach to controlling policies, depicted in Fig. 1, represents only a small extract of the holistic trust-architectural design concept depicted in Fig. 2, which was introduced in [9] and provides the evaluated base for policy expressiveness and transformation as part of a trust-establishment conceptualisation.

The dynamically established network consists of linked Trust Points, each Trust Point representing a Policy Authority from a regulation point of view. In comparison to social coupling, this kind of architecture claims regions of the cloud user's responsibilities and reflects his dynamically extended scope of regulation. Each established Trust Point acts as a single authority responsible for specific scopes of policy.

The provisioning of Trust Points establishes identifiable entities. The gate to all factors of trust management is the trust in identity [3]. Therefore, the assurance of a secure authentication of identity becomes essential. The process of establishing trustworthy entities has to be combined with the establishment of a cloud-user security context, the user's base of trust on the cloud system's premises. The establishment of a cloud-user security context requires new interfaces for mutual negotiations between user and provider. After a successful negotiation, the cloud user's scope of regulation is extended with the newly established base of trust.

Assuming that each Policy Authority has established a secure session with the central policy knowledge base, the assignment of policies to a specific Policy Authority is declaratively expressed through the method *targetToZone* and is linked to a domain-specific area. The architectural model depicted in Fig. 2 can potentially satisfy different trust-design requirements. The range of specific authorities can be separated, provides a base for modularisation, and enforces principles of separation of duty.

3.3 Trust-Establishment Protocol

The network of trust needs specific policies to regulate the establishment of Trust Points. Besides policies for deployment, actor cooperation, security, and privacy, the current work introduces a specific trust policy to provide a base of linked trusted entities for all further regulation purposes. Such expressivity allows the definition of specific trust policy, negotiating different levels of binding between the cloud user and his trustworthy entities.

The Trust-Establishment-Protocol (TEP) depicted in Fig. 2 is responsible for trust-condition negotiation, starting from a hardware-based root of trust. Once a root of trust is authenticated based on the trust policy, a security context is established through a Trust Point capable of enforcing cloud-specific policies in regard to this regulation layer. Before the next cloud layer can be

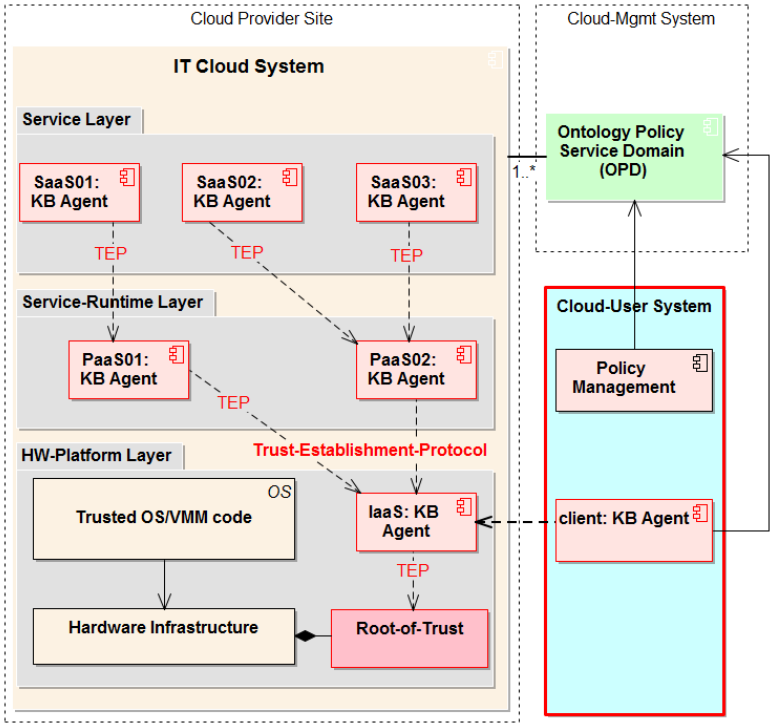

Fig. 2. Trust Points: Network of Policy Authorities

regulated, a fundamental security context has to established and, based on the Trust-Establishment-Protocol, the next trustworthy entity is linked to a chain of trust. The TEP is a cryptographic protocol and uses the TCG Software Stack (TSS) following the TCG version of the TSS specification [16]. The TEP is currently part of the Knowledge-based Agent development.

4 The Ontology Concept

The decision to apply an ontology comes from the demand for a formal representation of knowledge as a base for a precise semantic interpretation of the regulation, domain, and security aspects. Due to its reasoning capability, inferring plays a role for concepts like States, Trust, or Risk, all examples of a represented knowledge that can never be expressed explicitly but is derived from structural or security properties of a target system.

Descending from F-Logic, the ontology language ObjectLogic is used [10]. ObjectLogic extends classical predicate calculus with an object-oriented programming paradigm and follows the closed-world assumption for knowledge representation that assures stable conditions and system states of an expected real

world. The distributed architecture depicted in Fig. 3 treats the aspect of regulation, the target of regulation, and the aspect of security as separate conceptual frameworks.

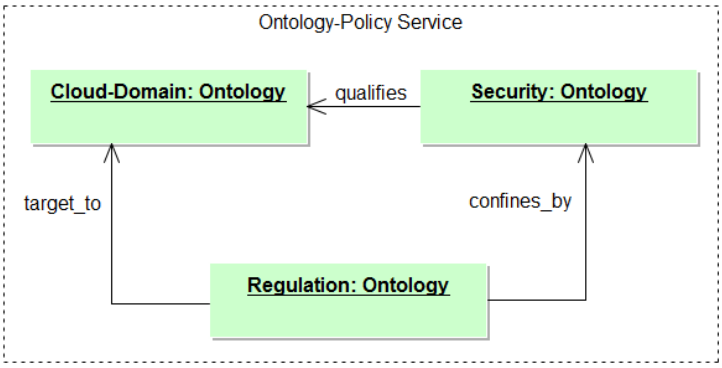

Fig. 3. Multiple-Ontology Architecture

Besides the regulation formalisation, the target of regulation, the public cloud, can be formally modelled using an axiomatic language introducing all required cloud concepts as domain vocabulary. From the architectural point of view, the ontology approach allows a system design in stages, starting from some required base concepts that can be formally engineered into more complex system concepts. Both ontologies are well-suited for the demonstration of the base principle in order to establish a structurally and behaviourally regulated concrete cloud system.

The security ontology extends the function-driven domain formalisation with quality-driven concepts like Assets, Confidentiality, and Availability, providing a foundation for the expression of these concepts in authenticated, integrity-protected, or encrypted states, for example [7],[6]. The current work extends the security consideration through a security-model conceptualisation. Security models provide a formal representation of the access-control security policy [13]. The use of a Mandatory Access Control (MAC) model mitigates deficiencies of standard UNIX-based access-control models; the cloud user is given the security background needed to take over responsibility for security management.

The distributed ontology design is still under development; it will be extended based on the evaluation results of the current Cloud-Kit proof-of-concept and will be published in a specialised paper about the conceptualisation approach.

5 The Cloud-Kit Reference Project

The idea of a Cloud Kit is modularisation: the cloud user is faced with a new role as designer of trustworthy cloud services as opposed to to his generally ac-

cepted service-consuming role, which is influenced by the Trusted Computing Group (TCG) specification standards [15] describing architectural submissions and processes to establish trusted multi-tenant infrastructures. The main concepts behind the design principles are the Trusted Context and the Trusted System Domain.

The distinction between cloud user and cloud provider remains, but their authorities are fully reviewed and redefined. The cloud user must now select the right conditions for his own architectural design of a cloud foundation commensurate with his compliance requirements. One of the cloud provider's responsibilities is the preparation of well-founded infrastructural environments for the cloud user's independently designed cloud-service concept.

The Trusted Context represents a verified cloud provider's identity and provides cryptographic key artefacts for further mutual negotiations between both parties, thus separating all communication from other cloud users on the same cloud platform. The usage of cryptographic keys for signing and encryption maintains the cloud user's confidence in his connection to the target cloud-provider platform and allows him to adjust the technical preconditions by computing cryptographically signed cloud-platform properties in regard to his base requirements.

The Trusted System Domain is a runtime home base equipped with instruments and controlling resources. Through the use of cryptographic artefacts, it is able to establish a secure channel between the cloud user and the Trusted System Domain.

The cloud architectural reference model was first introduced in [9] and enables the evaluation of a dynamically established interconnected Trust-Point backbone following the model in Sec. 3.2. Rooted in a trusted IT platform layer and reaching the service layer, different Trust Points control ontology-provided policies and trustworthily report the current trust and system state. The proof of concept should resolve the following points:

- **trust policy enforcement:** The proof of concept verifies the roll-out of policy agents based on TEP; they are responsible for policy enforcement and for providing technical interfaces to transform diverse regulation goals.
- **satisfiability of domain concept:** It is important to verify the degree of detail of each object's specification to model an arbitrary cloud architecture.
- **policy coverage:** The policy conceptualisation has to provide a generalisation able to express different governance objectives [14],[5] in order to control specific processing alignments.
- **policy expressiveness:** The concept of constraints largely determines the process of context-oriented regulation refinement. It is important to prove the expressiveness of the underlying constraint conceptualisation in regard to different levels of constraining aspects.
- **policy transformation capabilities:** Transformations induce costs in terms of duration, computing time, and synchronisation, so the question of transformation efficiency remains open.

6 Outlook

The current work demonstrates a fully new approach to cloud system management where trust is deliberately established as a foundation for the cloud user's regulation range, allowing the design of a user-defined cloud service environment.

The issue of the assured system state is currently under development. Once the cloud user can effectively enforce different policies, he needs confidence that the established system state will not change without his knowledge.

During the development of a powerful declarative regulation framework, contractually defined one-way policy control requires extended declarative concepts restricting the cloud provider from influencing running policies defined by the cloud user. Here it is important to integrate the support of different security models into the current regulation conceptualisation.

As part of the cloud-domain ontology, Connections are essential conceptual elements that establish the system state and deploy a horizontally driven relationship model. Each instance of a Connection affects both functional and security policy design.

The concept of Connections has to be extended to introduce the Trust-Establishment-Protocol (TEP) depicted in Fig. 2 and deploy a vertical relationship model. The protocol design is still under development but should become an integrated part of the Connection conceptualisation.

Successfully finalising both the support of extended security models and the regulated establishment of vertical trustworthy Connections provides the foundation for a user-defined cloud policy.

References

[1] Darko Androcec, Neven Vrcek, and Jurica Seva. "Cloud computing ontologies: a systematic review". In: *Proceedings of the third international conference on models and ontology-based design of protocols, architectures and services*. 2012, pp. 9–14.

[2] Prashant Barot et al. *Cloud Computing - Evolution in der Technik, Revolution im Business*. Ed. by Dr. Mathias Weber. BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., 2009.

[3] Messaoud Benantar. *Access control systems: security, identity management and trust models*. Springer Science & Business Media, 2006.

[4] BSI. *Sicherheitsempfehlungen für Cloud Computing Anbieter*. 2012.

[5] EUROPEAN COMMISSION. *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Tech. rep. EUROPEAN PARLIAMENT and OF THE COUNCIL, Jan. 2012. URL: `http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf`.

[6] Stefan Fenz and Andreas Ekelhart. "Formalizing information security knowledge". In: *Proceedings of the 4th international Symposium on information, Computer, and Communications Security*. ACM. 2009, pp. 183–194.

[7] Almut Herzog, Nahid Shahmehri, and Claudiu Duma. "An ontology of information security". In: *International Journal of Information Security and Privacy (IJISP)* 1.4 (2007), pp. 1–23.

[8] Thorsten Humberg et al. "Using Ontologies to Analyze Compliance Requirements of Cloud-Based Processes". In: *Cloud Computing and Services Science*. Springer, 2014, pp. 36–51.

[9] Jörg Kebbedies et al. "Conceptualized Policy Design for User-Regulated Trusted Clouds". In: *UCC 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing* (2015).

[10] Michael Kifer and Georg Lausen. "F-logic: A Higher-order Language for Reasoning About Objects, Inheritance, and Scheme". In: *Proceedings of the 1989 ACM SIGMOD International Conference on Management of Data*. SIGMOD '89. Portland, Oregon, USA: ACM, 1989, pp. 134–146. ISBN: 0-89791-317-5. DOI: 10.1145/67544.66939. URL: http://doi.acm.org/10.1145/67544.66939.

[11] Felix Kluge. "Entwicklung und Konzeption zur Umsetzung einer Transformation von einer ontologischen beschriebenen Policysemantik in eine sichere agentenbasierte Ablaufsteuerung". BSc thesis. Technische Universität Dresden, 2016.

[12] OASIS. "Topology and Orchestration Specification for Cloud Applications Version 1.0". In: *Organization for the Advancement of Structured Information Standards* (18 March 2013).

[13] Amon Ott. *Mandatory Rule Set Based Access Control in Linux: A Multipolicy Security Framework and Role Model Solution for Access Control in Networked Linux Systems*. Aachen, Germany, Germany: Shaker Verlag GmbH, Germany, 2007. ISBN: 383226423X, 9783832264239.

[14] G. Recht. *Bundesdatenschutzgesetz (BDSG) (German Edition)*. CreateSpace Independent Publishing Platform, June 2014. ISBN: 9781500100025. URL: http://amazon.com/o/ASIN/1500100021/.

[15] Trusted Computing Group. *TCG TMI Reference Framework*. 2013.

[16] Trusting Computing Group. *TCG Software Stack Specification*. Mar. 2009. URL: http://www.trustedcomputinggroup.org/resources/tcg_software_stack_tss_specification.

[17] Lamia Youseff, Maria Butrico, and Dilma Da Silva. "Toward a unified ontology of cloud computing". In: *Grid Computing Environments Workshop, 2008. GCE'08*. IEEE. 2008, pp. 1–10.