Accountability for Service Compliance: A Survey

Jinhui Yao, CSIRO ICT Centre, Australia, and University of Sydney, Australia
Shiping Chen, CSIRO ICT Centre, Australia
David Levy, University of Sydney, Australia

ABSTRACT

In recent years, a range of innovations in the ‘service’ related technologies have been witnessed, namely SaaS, PaaS, and IaaS. Meanwhile, Service Oriented Architecture (SOA) enables composing different services seamlessly to form new service network. The combination of the two trends allow individual organizations to overcome their limitation of computing resources and obtain the maximum value of the functionality themselves can provide. One major issue with such massive composition is to verify the compliance of participating entities. Composed services usually span several administrative domains, where each has its own priorities. Given the fact that an admission to a violation may cause penalties, it is conceivable that an entity may intend to deceive. To tackle this issue, ‘accountability’ has emerged as a promising concept to achieve system trustworthiness. Recently, accountability has received considerable attention in research communities, and many approaches have been proposed. In this survey, the authors discuss the concept and desirable properties of accountability, clarify the requirements and differences that distinguish accountability to other related approaches, and systematically summarize and evaluate various approaches of accountability.

Keywords: Accountability, Compliance Assurance, Service Oriented Architecture (SOA), Survey, Trustworthiness

INTRODUCTION

In recent years, we have witnessed a range of innovations in the ‘service’ related technologies and concepts. Following the Software as a Service (SaaS) paradigm, two other ‘as a service’ paradigms have been proposed. They are Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The widespread adoption of these paradigms strongly suggests the possibility and practicality of encapsulating and providing any type of technological product as a service.

On the other hand, Service Oriented Architecture (SOA) enables us to combine different services provided by different service providers seamlessly to form new service network. The SOA design paradigm has been widely adopted by organizations striving to attain flexibility in their business, either by offering their own

DOI: 10.4018/jssoe.2012010102
services to others, or offering new value added services through combining of their proprietary services with those offered by third parties (Papazoglou, 2007).

The combination of the two trends effectively evolved the notion of the distributed computing. Applications, platforms, infrastructures, as well as services provided by different vendors from different locations can now be conveniently brought together to become a unified system for specific tasks. This allows individual entities to overcome their limitation of computing resources and obtain the maximum value of the core service they can provide. This type of massive service composition is now often referred to as ‘organization mash-up’.

Whilst such paradigm provides many benefits, it inevitably introduces certain issues, such as compliance of the participating entities. In such composition, each of the participants would behave according to the predefined and mutually agreed upon business logic and Service Level Agreement (SLA). As far as the participants are in the collaboration, the correctness of the system operation depends on: firstly, that the agreement and logic are correct, and secondly, that each participant complies to them at all times. Any deviation from this agreement is regarded as a violation, and a robust mechanism for maintaining participant actions, in accordance with the respective business logic and SLA, is critically essential for such paradigm to be practically viable.

However, the detection and prevention of failures in a collaborative environment is complicated by the fact that the resultant system usually spans several administrative domains, each with its own interests and priorities. Given the fact that an admission to a violation may incur penalties in some form, it is conceivable that an entity may intend to conceal its fault. This represents a great challenge and obstacle for this collaboration to take place in practice.

Recent study of this issue has raised awareness that instead of conventional correctness assurance, trustworthiness plays a more important role in this scenario. Building on the notions of trust presented, a trustworthy system (IETF, 2007) is defined as: a system that is already trusted, and continues to warrant that trust because the system’s behaviors can be validated in some convincing way.

To achieve trustworthiness, the concept of ‘accountability’ emerged. Accountability refers to the ability of the system to be trustworthy, in another words, strong accountability implies that the system can show its compliance unambiguously and convincingly. In past few years, the research community has proposed many accountability concepts and approaches to target this issue. Whilst the research on accountability is still rapidly developing, it is a good time to discuss the concept and desirable properties of accountability, clarify the requirements and differences that distinguish accountability from other related concepts, and systematically summarize and evaluate various approaches of accountability. This survey aims to achieve this goal.

In next section, we will first discuss accountability as a concept and its essence. Taxonomy is provided at the end of the section, according to which, different research works in the area will be overviewed in the remaining sections. Finally, we conclude with a summary and discussion of future research directions.

**OVERVIEW OF THE CONCEPT**

Over decades, the concept of accountability has been intensively studied by researchers in various disciplines; many intended to interpret it in their own terms. Those interpretations are sometimes complementing, and sometimes extending each other. In this section, we will overview some of those works aimed to answer this very basic question: What is accountability? And what are its implications within modern day computing or service based systems.

**Accountability in Social Science and Governance**

The use of the term accountability to describe a feature of service systems was not common until recent years, when the technology has
Innovating Healthcare through Remote Monitoring: Effects and Business Model
[www.igi-global.com/article/innovating-healthcare-through-remote-monitoring/144814?camid=4v1a](www.igi-global.com/article/innovating-healthcare-through-remote-monitoring/144814?camid=4v1a)

Calculating Quantitative Integrity and Secrecy for Imperative Programs
[www.igi-global.com/article/calculating-quantitative-integrity-and-secrecy-for-imperative-programs/136465?camid=4v1a](www.igi-global.com/article/calculating-quantitative-integrity-and-secrecy-for-imperative-programs/136465?camid=4v1a)