CORA Cork Open Research Archive
Cartlann Taighde Oscailte Chorcaí

Title	A trust label system for communicating trust in cloud services
Authors	Emeakaroha, Vincent C.;Fatema, Kaniz;van der Werff, Lisa;Healy, Philip;Lynn, Theo;Morrison, John P.
Publication date	2017
Original Citation	Emeakaroha, V. C., Fatema, K., Werff, L. v. d., Healy, P., Lynn, T. and Morrison, J. P. (2017) 'A Trust Label System for Communicating Trust in Cloud Services', IEEE Transactions on Services Computing, 10(5), pp. 689-700. DOI: 10.1109/TSC.2016.2553036
Type of publication	Article (peer-reviewed)
Link to publisher's version	https://ieeexplore.ieee.org/document/7457329 - 10.1109/TSC.2016.2553036
Rights	© 2017 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
Download date	2026-11-01 08:17:24
Item downloaded from	https://hdl.handle.net/10468/8405

UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2016.2553036, IEEE Transactions on Services Computing

A Trust Label System for Communicating Trust in Cloud Services

Vincent C. Emeakaroha, Kaniz Fatema, Lisa van der Werff, Philip Healy, Theo Lynn and John P. Morrison

Abstract—Cloud computing is rapidly changing the digital service landscape. A proliferation of Cloud providers has emerged, increasing the difficulty of consumer decisions. Trust issues have been identified as a factor holding back Cloud adoption. The risks and challenges inherent in the adoption of Cloud services are well recognised in the computing literature. In conjunction with these risks, the relative novelty of the online environment as a context for the provision of business services can increase consumer perceptions of uncertainty. This uncertainty is worsened in a Cloud context due to the lack of transparency, from the consumer perspective, into the service types, operational conditions and the quality of service offered by the diverse providers. Previous approaches failed to provide an appropriate medium for communicating trust and trustworthiness in Clouds. A new strategy is required to improve consumer confidence and trust in Cloud providers. This paper presents the operationalisation of a trust label system designed to communicate trust and trustworthiness in Cloud services. We describe the technical details and implementation of the trust label components. Based on a use case scenario, an initial evaluation was carried out to test its operations and its usefulness for increasing consumer trust in Cloud services.

Index Terms—Service Monitoring, Trustmark, Cloud Services, Data Location, Trust Label, Cloud Computing, Trustworthiness

1 Introduction

Cloud Computing is rapidly transforming the IT and service provisioning landscapes. It facilitates new methods of improving digital services and their means of consumption. Gartner (2015) [1] describe Cloud Computing as the foundation of digital business, as it encourages and facilitates new methods of delivering digital services to consumers. Predictions of the market size of the global Cloud Computing industry estimate that it will reach U.S $241 billion by 2020 [2]. As a result, Cloud Computing has become a key component of IT and business strategy, combining the benefits of IT efficiency and business agility [3]. It offers numerous benefits to consumers including: economy of scale, on-demand resource provisioning, and a pay-as-you-go billing model that replaces capital expenditure with operational expenditure [4].

Cloud services comprise different layers of resources, ranging from infrastructure at the lowest layer to software applications at the highest. The advantages of Cloud Computing include immediate access to hardware resources, lower IT barriers to innovation, easier scaling for service provisioning and lower cost of entry for small firms engaged in compute intensive tasks [3]. Despite these significant advantages, the adoption of Cloud Computing has come up against a number of barriers such as data jurisdiction and location, security and trust, portability and technology transparency, business-related barriers and industrial policy [5]. Among these barriers, consumer trust has been considered a major hinderance to Cloud uptake due to the large-scale and abstract nature of Cloud services [6], [7]. Consumers lack insight into Cloud service operations and as a result find it difficult to trust them. In addition, the impact of trust on adoption of, and interaction with, information communication technology is widely established [8], [9], [10]. Experts in the field argue that the biggest impediments to Cloud adoption are likely to be attitudinal rather than technological [11]. This suggests that researchers should take a holistic approach to the study of Cloud adoption, incorporating considerations of consumer attitudes alongside technological advances.

In a Cloud environment, trust may be hampered by uncertainty related to features of the product itself, alongside risks associated with the Internet context [12] and those posed by malicious third parties [13], [14]. The situation is complicated further by the relative novelty of online services, a lack of consumer understanding, and the sheer number of unknown providers offering these services [7]. Attempts to allay these fears have taken a range of forms including aesthetic design of websites, feedback reputation systems and third party endorsements [15].

In our previous paper, Lynn et al. [7] introduced a Cloud trust label system as a mechanism for communicating Cloud service trustworthiness online. While the label shows promise for increasing transparency for consumers and trust in Cloud services, how the features of the label might be operationalised and measured in real time has yet to be explored. This paper builds on and extends that work to provide a description of the trust label system, the technical implementation and a demonstration of its usage in a Cloud service provisioning scenario. In particular, we focus on two aspects of the trust label - data management and metrics monitoring - to provide an in-depth investigation of how these features can best be operationalised. The main contributions of this paper are (i) technical descriptions of the

- *V C Emeakaroha and P Healy and J P Morrison are with IC4 University College Cork, Ireland.*
- *K Fatema is with Trinity College University Dublin, Ireland.*
- *L van der Werff and T Lynn are with IC4 Dublin City University, Dublin Ireland.*

1939-1374 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2016.2553036, IEEE Transactions on Services Computing

trust label system and its operationalisation; (ii) the design and implementation of a data location model to manage and inform consumers of their data location in Clouds; (iii) the design and implementation of a service monitor framework that monitors Cloud services at run-time and updates the information displayed by the trust label interface and (iv) the evaluation of the trust label system using a real world use case scenario to demonstrate its practical usefulness. In doing the evaluation, we take a holistic, cross-disciplinary approach to exploring the issues of consumer trust in Cloud services.

The rest of the paper is organised as follows: Section 2 presents some theoretical literature on trust in Cloud computing environment and highlights its challenges. In section 3, we discuss the previous work that are related to ours and thereby differentiate them to show the novelty of our contributions. Section 4 described the proposed trust label system and its operationalisation efforts. In addition, we describe the design and implementation of its components. Section 5 presents the evaluations based on a use case scenario and the achieved results. In Section 6, we conclude the paper and highlight our future work.

2 Trust in Cloud Computing

Trust is a psychological state which involves a willingness to be vulnerable to another party based on positive expectations of the future behaviour of that party [16]. Trust is particularly relevant in situations where uncertainty is high, vulnerability is difficult to control, the relationship between parties is long term and interdependent and the risks associated with failure are high [17]. Relationships between Cloud service consumers and providers tend to feature all four of these characteristics. Specifically, consumers typically look to service providers for long term service provision to support business activities that are vital to the functioning of their organisation. This service is provided using a distributed network where consumer knowledge of the functioning and security of the network is often limited. In contexts such as these, trust is likely to be a vital ingredient in facilitating a relationship between the service provider and the consumer.

In a Cloud context, trust has been described as a three stage process which consists of consumer perceptions of Cloud services and their providers, a decision to trust those services, and Cloud adoption behaviour such as purchasing [7]. Within this process, trust has three important potential referents: trust in the Cloud provider; trust in the Cloud service; and trust in the Cloud itself. Trust in the Cloud provider could concern the ability to honour established agreements with consumers, for example, Service Level Agreement (SLA), which specifies quality obligations such as acceptable uptime value. Trust in the Cloud service may relate to the ability of the service to perform the intended objectives. This could be evaluated based on consumer satisfaction and historical usage data. Trust in the Cloud itself seems to be the most difficult since it deals with the act of convincing users to adopt Cloud as a technology. Clearly differentiating between these different referents of trust is an important step in establishing how trust can be built in the context of interaction with technology [18], [19]. The primary discussion of trust in Cloud computing is around calculus based trust [20], for example monitoring the potential cost and benefits of adopting a particular technology. However, by design, it is suspicious, bureaucratic and transactional.

A variety of methods have been devised to influence consumer perceptions of Cloud services. Perceptions of another party which are likely to influence trust are known as trustworthiness and can be organised according to three categories [8], [21], [22]: The first category includes competence, functionality or performance relating to perceptions that the Cloud service is capable of allowing the consumer to achieve their goals. The second category includes benevolence or helpfulness perceptions relating to feeling that support is available in using the service. Finally, predictability and reliability perceptions are based on beliefs that the service will be dependable and function in a predicable manner. Realistically, any individual Cloud service provider can aim to directly influence these trustworthiness perceptions in terms of trust in the Cloud provider and trust in the Cloud service. Attempts to do so are also likely to have a spillover effect in terms of trust in the Cloud in general, although this may be a more long term proposition. Cloud service providers who successfully communicate trustworthiness characteristics to consumers have the advantage of building knowledge based trust with their customers. Knowledge based trust is argued to represent the threshold between suspicion and positive expectations and as such is often seen as the starting point of real trust [23]. Knowledge based trust relationships have the advantage of being accompanied by less suspicion and monitoring and tend to be more robust than those built on trust which is informed by a simple calculation of risks versus benefits (i.e. calculus based trust) [20]. As such, building knowledge based trust with consumers should be a key priority for Cloud service providers. Therefore, we aim to address this challenge in this paper.

3 Trust Challenges and Related Work

The trust challenges raised by the emergence of Cloud computing are similar to those raised by the Internet at a whole. Consumers of Cloud computing, similar to general Internet consumers must trust that Cloud providers will deliver the agreed quality of service, securely store their data and respect their privacy [24]. In the Internet, trustmarks, which are any third-party mark, picture or symbol, have been used in an effort to dispel consumers' concerns regarding risk and therefore increase their trust [25]. Recipients of trustmarks are typically subjected to a manual verification and certification process that varies among the trustmark issuing sectors and is not transparent to consumers. Therefore, the approach is open to criticism regarding accuracy, consistency, timeliness, transparency and ease of abuse [26]. Based on the static and passive forms of trustmarks, they cannot be effectively used to address the trust and confidence issues in Cloud computing due to the mostly dynamic nature of Cloud services. As a result, a more active and dynamic approach is required for providing trust information for Cloud consumers. The Cloud Security Alliance (CSA) Security Trust & Assurance Registry (STAR) is a method designed for providing security assurance certification in

1939-1374 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2016.2553036, IEEE Transactions on Services Computing

Clouds. It certifies and assures the compliance of Cloud provider security practices to consumers. Notwithstanding this, such assurance (and associated trustmarks) have been subject to criticism for being (i) largely reliant on human intervention (with limited capacity), (ii) limited in scope, (iii) passive, periodical and retrospective, (iv) lacking warranties and (v) subject to co-optation risk [25]. More recently, CSA STAR is working to integrate continuous monitoring in an effort to alleviate some of those criticisms and to automate the certification process. This shows the importance of flexible monitoring for such systems and it clearly relates to our operationalisation approach in this paper for the trust label system, which covers a broader spectrum of Cloud service metrics other than security. The CSA CloudTrust Protocol (CTP) presents a similar mechanism for managing Cloud service security to improve consumer trust. However, security controls are only one part of the wider fabric that makes up trust and thus a security-oriented perspectives does not capture the wider complexity of how trust is formed, maintained or lost. The CTP API can be integrated with the trust label system to push security measurements to the label interface. However, further work would be needed to explore those security measurements and validate whether they in fact either build trust or contribute to trust and at what level. At the moment, there is an open question on how CTP could be consumed by consumers and enterprise buyers. We argue that it can be made consumable by integrating it with the trust label system.

Furthermore, Cloud computing, like digital business ecosystem built on chains of service provisions, present various issues that can impair trustworthiness and dependability. These encompass data provenance, technology implementation and operation transparency and the predictability of a technology to behave within expected norms, that is, dependability [27]. Strategies to address these issues in Cloud computing may include new approaches to constructing dependability arguments; methods and tools for testing Cloud infrastructures and configurations; self-aware systems that make information about their operation and failure available for scrutiny and use; and regulatory and social mechanism to highlight dependable and trustworthy service providers [27]. These strategies however, need to be formally defined and operationalised.

Existing research has focused predominantly on how the trustworthiness concept can be applied to consumer trust in technology providers or institutions. Thus far, communication of trustworthiness online has tended to take the form of website design characteristics, reputation feedback mechanisms or third party endorsements. Researchers exploring the role of website design in communicating trust have suggested that online trust can be enhanced through the use of particular visual aesthetics including particular colour tones, brightness levels, and graphics effects [28]. Furthermore, related design issues such as ease of navigation also appear to play a role [29], [30]. In contrast, reputation feedback mechanisms are proposed to impact trust perceptions by providing a third party rating of behaviour in previous transactions as well as signalling to the consumer that participation in such mechanisms offers a potential deterrent for untrustworthy behaviour in future transactions [31]. Empirical evidence demonstrates that consumers often view these recommendation systems as social actors and reliance on their information depends on the consumer perceptions of the recommendation system's ability, benevolence and integrity or their less personal equivalents e.g. performance, helpfulness and predictability [32], [33]. Finally, third party endorsements may take the form of certifications, security seals, privacy seals and business identity seals [34], [35] and are designed to provide consumers with additional information about the transmission of data, use of privacy policies and reputation of the business. Aiken *et al.* [24] argue that this form of third party endorsement is effective in increasing trust above and beyond any influence of recommendation systems.

Unfortunately, the impact of each of these methods on trust has been mixed. For instance, trust inducing website aesthetics have been shown to vary across gender and culture [36], [37], the applicability of reputation systems for long term service provision is questionable and many consumers appear to be unaware of the presence of third party seals when making trust decisions [38], [39]. In the Cloud environment, reputation tools and third party endorsements are impractical for many service providers given the size of their existing customer bases and the absence of an independent quality assurance body [40]. Accountability measures has been proposed as a potential means of addressing the lack of trust and confidence in Cloud service offerings [41]. This approach includes preventive actions and it has the character of assigning liability in case of failure through detective measures. It does not however provide information on the dependability and predictability of Cloud services, which are essential to develop consumer trust. Assurance is different to accountability. It deals with conclusions by practitioners designed to improve the degree of confidence of the intended users and not the responsible party about the outcome of an evaluation of a subject matter against criteria [40]. One may argue that it is not initially focused on failure and liability rather on dependability and possibly predictability. Assurance brings many benefits such as an independent opinion from an external source that enhances the credibility of a Cloud service and reduction of perceived management bias in service claims. Therefore, an integrated approach to accountability and assurance has been encouraged for Cloud computing [40].

Previously, we use a panel of Cloud industry experts engaged in a Delphi process to develop a Cloud trust label interface, which aims to provide consumers with information about Cloud services on which they can base their trustworthiness perceptions [7]. The paper detailed the Delphi process for creating the trust label however, it neither discuss the practical implementations or present usage examples of such a trust label system, which are essential for its operationalisation. In this paper, we discuss the proposed trust label system, present its technical implementations to operationalise it and demonstrate its practical usage.

4 Trust Label System

The trust label system presented here was developed through a Delphi methodology. The Delphi method can be characterised as a *method for structuring group communication to allow the discussion and joint resolution of a complex problem*

1939-1374 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2016.2553036, IEEE Transactions on Services Computing

[42]. Figure 1 presents the trust label interface derived using this process. As shown in the figure, the interface specifies a range of important metrics, which Delphi participants felt were necessary for communicating trustworthiness to Cloud consumers. Further details on the Delphi process for creating this trust label can be found in [7].

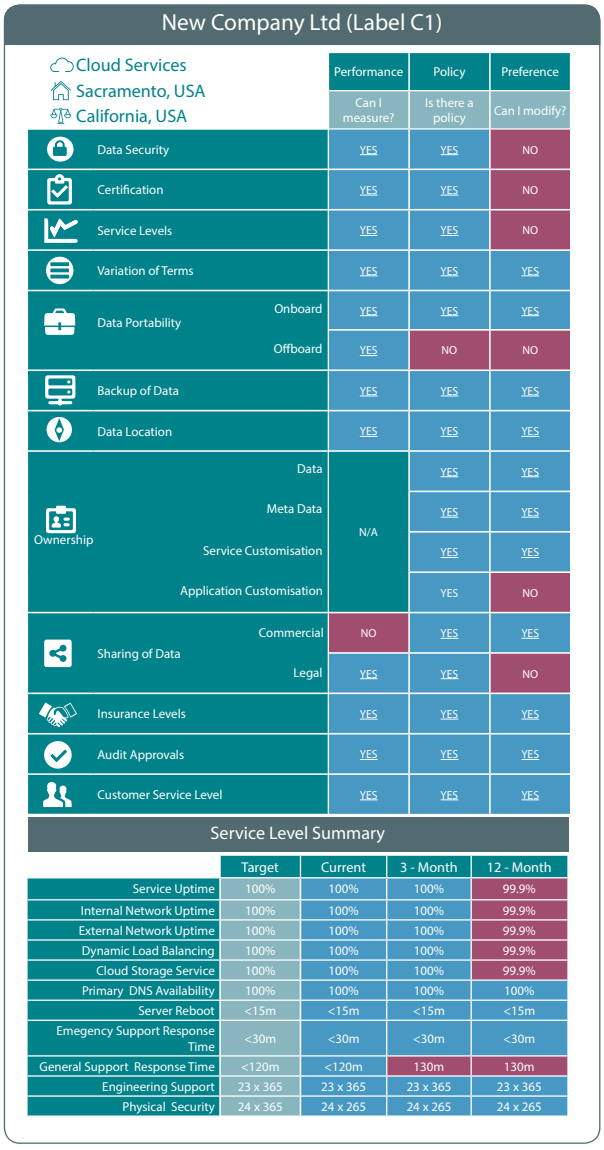


Figure 1. Trust Label Interface

The trust label system addresses multiple levels and controls in Clouds. Its interface, presented in Figure 1, is divided into two key parts - (i) the main section and (ii) the service level summary. In addition, at the top of the label, details of the Cloud service provider including name, address and jurisdiction are displayed for the consumers.

The information presented in the main section of the trust label is organised (as shown in Figure 1) according to whether it relates to the ability to measure a metric (Performance), the Cloud service provider's policy regarding a metric (Policy), and the extent to which the consumer can specify preferences for how a metric is dealt with (Preference). The value specified for the performance, policy and preference options of each metric are designed to provide pop up links, which give further information or clarification for the value.

The main section of the trust label consists of composite metrics that can be classified into three metric groups - (i) service execution, (ii) data management and (iii) contract condition. Table 1 summarises the classification.

Table 1
Composite Metric Classification

Service Execution	Data Management	Contract Condition
Service Levels	Data Security	Certification
Customer Service Level	Data Portability	Variation of Terms
	Backup of Data	Insurance Levels
	Data Location	Audit Approvals
	Ownership	
	Sharing of Data	

The service execution metric group contains the parameters to describe a Cloud providers operational performance. The data management metrics include the parameters to inform consumers about the Cloud providers data management strategies. The contract condition metrics explain the requirements based on which consumers could trust contracts entered into with the Cloud provider.

The service level summary part of the trust label interface includes further details that describes the *Service Levels* composite metric identified in the main section.

This paper focuses on the operationalisation and demonstration of the service execution and data management metric groups. The contract condition metric group will be considered in a future work.

In the following sections, we explore the technical issues that relate to the operationalisation of the service execution and data management groups' metrics to inform a dynamic trust label system.

4.1 Data Management Metrics

Data management is one of the key challenges hindering consumer adoption of Cloud services. In this regard, consumers are often concerned about the location, security and usage of their data and a lack of transparency surrounding these issues. To mitigate this worry, the trust label system includes four composite metrics to transparently surface information to consumers regarding the management of their data in order to establish trust. The metrics are: *Data Security, Data Portability, Backup of Data, Data Location, Ownership* and *Sharing of Data*.

In this group, we use the data location metric as an example to demonstrate the operationalisation process. In the following sections, we describe how the values for the three options (*Performance, Policy, Preference*) were achieved for this metric.

4.1.1 Data Location Performance

The value of the "performance" column on the trust label interface indicates whether the consumer can measure the metric. In the case of data location, the measurement of performance surfaces whether the consumer can see the

1939-1374 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2016.2553036, IEEE Transactions on Services Computing

location of his/her data or not. The embedded pop up link in this value takes the consumers to an interface where they can check the location of their personal data. We developed this technology to give consumers visibility into the location of their personal data. It is underpinned by a data location control model for Cloud services [43]. Consumers can choose the locations for his/her data and the chosen location preferences are converted into XACML policy, which is consulted during every access to each item of personal data. To verify the provider compliance with the consumer location preference, the control model periodically evaluates the location information in the metadata and log entries. It notifies the consumer if there are variations. The location of consumer data is kept in a region information table. Each consumer can access the region information for his/her data after being authenticated as the data owner.

4.1.2 Data Location Policy

The "policy" value for the data location metric indicates whether there is a policy for choosing the location of a consumer data or not. The location control model manages the set of policy constraints specified for a data location. It allows each consumer to choose preferences for his/her data locations. The embedded link with this value takes the consumers to the interface where they can see the policy guiding their own data location in a chosen format. The consumer has to pass an authentication step before reaching this stage.

4.1.3 Data Location Preference

The "preference" value of the data location composite metric informs the consumer whether there is an option to modify previous configurations. In this case, the embedded link takes the consumers to the interface where they can modify their policy for the location of their data. Figure 2 presents a graphical illustration of this interface.

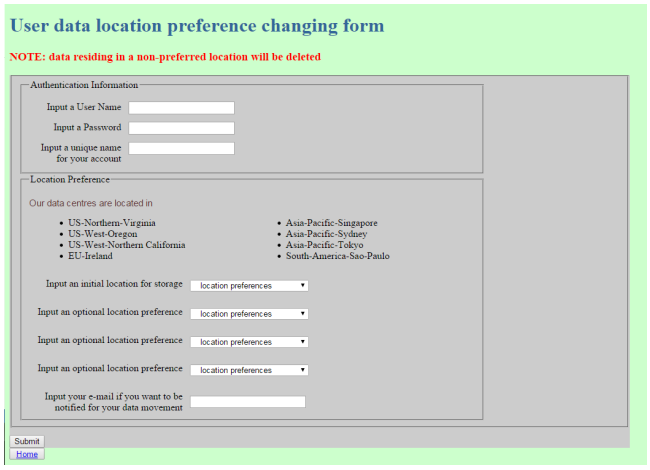


Figure 2. Preference Option Interface for the Data Location Metric

As discussed in a previous work [43], consumer policy is stored in the policy repository. Each of the policy is identified by a policy identifier (policy ID) and the corresponding data is identified by a data identifier (data ID). A link is maintained between the data ID and policy ID to identify which policy governs which data. When a policy is updated by changing preferences, it replaces the previous policy but keeps the same policy ID so that the link between the data and the policy remains unchanged. In addition, when policy preferences for a data location are changed, if there is any data already residing in a non-preferred location, that data is deleted.

4.2 Service Execution Metrics

The composite metrics in this group as shown in Table 1 are *Service Levels* and *Customer Service Level*. They describe the performance of a Cloud provider services.

The service level summary part of the trust label interface as shown in Figure 1, presents the details of the Service Levels composite metric. Therefore, we use this metric to demonstrate the operationalisation of this group. In this demonstration, we focus on how the service levels composite metric element values are being measured instead of describing it in terms of the option columns (performance, policy and preference) as done for the data location composite metric. The service level summary presents the element metrics and their values are dynamically updated at runtime to provide up-to-date information to consumers. The service level summary displays also 3- and 12-months average historical performance data of these elements.

To achieve the continuous updating of these element metrics, we present a service monitoring framework that monitors the Cloud services at run-time and surfaces the monitored values to the trust label interface.

4.2.1 Service Monitor Framework Design

The service monitor framework is a composite monitoring platform consisting of independent configurable monitoring tools that are managed in a decentralised manner. It is a holistic framework capable of monitoring both at the infrastructure and application levels in Clouds. Since many of the Cloud services today are application based, a resource-monitoring tool like *LoM2HiS* [44] would not be capable of monitoring all aspects of such deployments. Figure 3 presents the service monitor framework architecture.

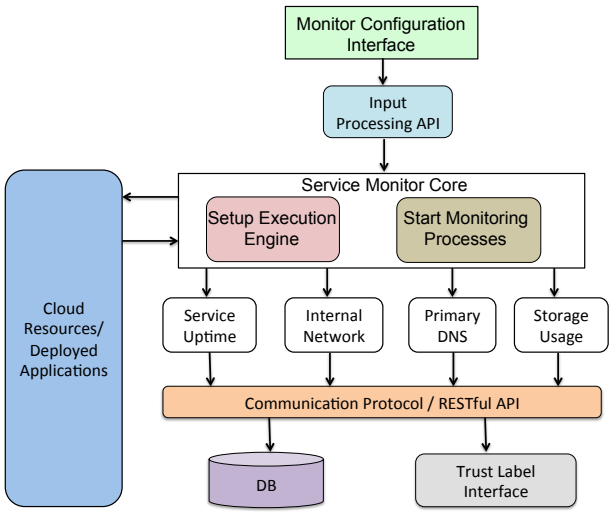


Figure 3. Service Monitor Framework Architecture

1939-1374 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2016.2553036, IEEE Transactions on Services Computing

As shown in Figure 3, the service monitor framework consists of different components that work together to achieve its objectives. The Monitor Configuration Interface is the front-end component for configuring the monitoring tools. It allows the parameterisation of the individual monitoring tools, for example to specify different monitoring intervals, and also the selection of particular monitoring tools for different purposes.

The Input Processing API gathers the configurations created using the front-end component and parses them into a suitable format for the back-end service monitor core engine to understand. It is the responsibility of the Service Monitor Core to instantiate the necessary monitoring tools with the proper configuration parameters and to co-ordinate their execution while they monitor the Cloud resources and deployed applications. The monitoring tools are executed in parallel and each sends its monitored data using the communication protocol into a database as well as to the trust label interface.

This monitoring framework is designed with quality in mind. We strive to make it non-intrusive, scalable, interoperable and extensible. These qualities have been described as important features of an efficient monitoring tool in a recent published monitoring survey [45]. Intrusive software is one that consumes significant resources on the monitored system, which may degrade the performance. Therefore, to achieve non-intrusiveness in our monitoring framework, we host the monitoring software on separate nodes to the ones used to run the Cloud services. However, we deploy a small agent on the computing nodes hosting the Cloud services to collect the monitoring information and send data back to the monitoring nodes. This separation of responsibility also increases the scalability of the monitoring tool since it facilitates the creation of clusters of monitoring agents with decentralised control nodes. We further enhance scalability by using distributed strategies coupled with efficient database technology to manage the monitored data.

Interoperability is another essential feature for a monitoring tool to be usable in heterogeneous Cloud platforms. In our service monitor framework, we used standardised data interchange formats to achieve neutrality in serialising and formatting the monitored data. Furthermore, we developed platform-independent communication mechanism based on message bus and HTTP protocols to facilitate seamless transfer of data between diverse Cloud platforms.

Extensibility describes the ability to easily customise and extend a software system. This is an important feature since Cloud computing is still evolving and many users have particular needs that cannot be covered by out-of-the-box software tools. To implement this requirement, a modular strategy was followed when designing the service monitor framework. This allows the organisation of the framework components into loosely coupled modules. Each of the modules embodies a unique function. Based on this strategy, it is easy to add new modules or extend an existing one without having to rebuild the entire service monitor framework.

In the operations of the service monitor framework, it directly updates the "Current" column in the service level summary section of the trust label interface as shown in Figure 1. In the next section, we discuss the mechanism for updating the "3-Month" and "12-Month" columns.

4.2.2 Running Average Calculation Mechanism

The data values in the "3-Month" and "12-Month" columns of the service level summary are calculated as running averages based on the current state of the monitored data. Figure 4 depicts a graphical illustration of the mechanism.

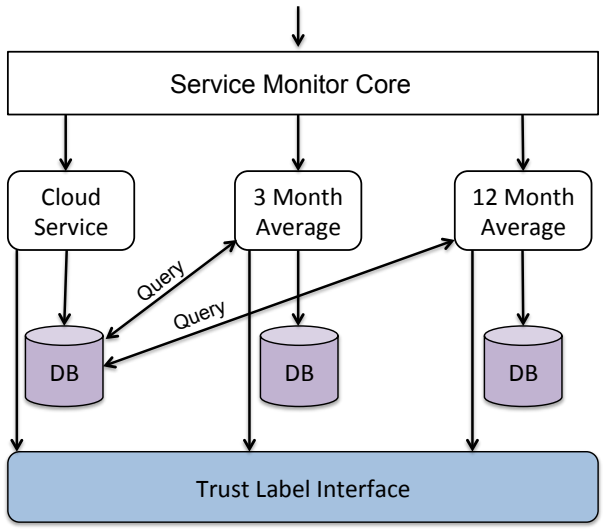


Figure 4. Average Calculating Mechanism

Independent processes perform the running average calculations. This mechanism is part of the service monitor framework. The Service Monitor Core engine is responsible for configuring, starting and managing these processes. Each of the monitored element metrics is designed to have separate "3-Month" and "12-Month" average calculating processes. As shown in Figure 4, the averaging processes query the Cloud service database to access the historical current monitored data, which are used in the calculations. The calculated values are continuously sent to the trust label interface using the communication protocol.

4.2.3 Service Monitor Framework Implementation

The Monitor Configuration Interface was developed using Ruby on Rails. The Ruby on Rails technology enabled quick development of this application and makes it compatible with other components. One of the attractive features of Ruby on Rails is its support for modularity. We exploited this feature to make the interface easily extendible with new functionality. Ruby on Rails provides many libraries and based on this, we used the JSON library to aggregate the inputted configuration data before transferring them down to the next component.

The Input Processing API component is implemented as a RESTful service in Java. Since Ruby on Rails supports RESTful design, it integrates seamlessly with this component in passing down the input data. The input processing API extracts these data and makes them available to the service monitor core component.

The Service Monitor Core component is implemented using the Java programming language. It sets up and manages the execution of a user selected and configured monitoring tools. In this component, we use multi-threading to achieve parallel execution of the monitoring tools. The

1939-1374 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2016.2553036, IEEE Transactions on Services Computing

monitoring tools are developed as individual application. When a user wants to run a particular set of monitoring activities, the service monitor sets up the appropriate tools based on the provided configuration parameters and manages application execution.

The interaction of the monitoring tools with the Cloud resources or deployed application is based on the type of monitoring objective that they aim to fulfil. For example, a resource monitoring tool is designed to gather the low-level resource utilisation information from, e.g., a Linux */proc* directory. In this case, the monitoring tool acts as an agent that resides on the targeted Cloud resource and parses files on that system to extract data such as CPU, memory and storage utilisations. However, in our solution, we implement an application-level monitoring tool to interact remotely with the target application and not reside on the same machine. In this approach, we use a *ping* mechanism to periodically query the status of the service. For HTTP queries, Java and .Net APIs was used.

Each monitoring tool incorporates communication protocols for transferring the monitored data to other components and for sending data to the trust label interface. The communication protocols comprise of a messaging bus that is based on RabbitMQ [46], HTTP protocols and RESTful services. This combination is aimed to achieve interoperability between platforms. To achieve scalability, the monitoring tools use a MySQL database cluster. Each instantiated monitoring tool is automatically assigned a database for persisting its monitored data. Hibernate is used to realise the interaction between the Java classes and the database. With Hibernate, it is easy to exchange database technologies. Thus, we are not bound to the MySQL platform and could easily exchange it with other ones.

The running average calculations are implemented as individual Java classes for each of the monitoring tools. Once a monitoring process is started for an element metric, the corresponding average calculators are automatically registered with a timer task. The timer task executes these averaging processes based on pre-configured time intervals. The calculated results are sent to the trust label interface using the communication protocols.

5 Evaluation

The trust label system is evaluated with the help of a use case scenario. We demonstrate the realisation of the data location and service level composite metrics. First, we present the evaluation environment and the use case scenario.

5.1 Evaluation Environment Setup

To setup the experimental environment, an OpenStack Cloud platform installation running Ubuntu Linux is used. The basic hardware and virtual machine configurations of our OpenStack platform are shown in Table 2. We use the Kernel-based Virtual Machine (KVM) hypervisor for hosting the virtual machines.

As shown in Table 2, the physical machine resources are capable of supporting on-demand starting of multiple virtual machines for hosting different Cloud services. An integrated load balancer is responsible for balancing the service requests in order to maintain high performance of the platform. The use of the OpenStack platform as the evaluation environment provides interoperability assurance of our approach.

Table 2
Cloud Environment Hardware

Machine Type = Physical Machine

OS	CPU	Cores	Memory	Storage
OpenStack	Intel Xeon 2.4 GHz	8	12 GB	1 TB

Machine Type = Virtual Machine

OS	CPU	Cores	Memory	Storage
Linux/Ubuntu	Intel Xeon 2.4 GHz	1	2048 MB	50 GB

5.2 Use Case Scenario Assessment

We present a use case scenario involving a consumer (broker) who is intending to buy Cloud services from a Cloud provider in order to offer them to its users in an end-to-end manner. The consumer has trust issues about Cloud services due to lack of knowledge and insight into their operations. We play the Cloud provider role and our objective is to communicate trustworthiness information to this consumer to neutralise these concerns. Figure 5 illustrates the end-to-end Cloud service provisioning setup. As can be observed in this figure, there are many components and points of failure that could pose problems for consumer satisfaction and accessibility of a service. Therefore, providing insight into these operations is essential to establish trust and encourage the consumer to adopt a Cloud service.

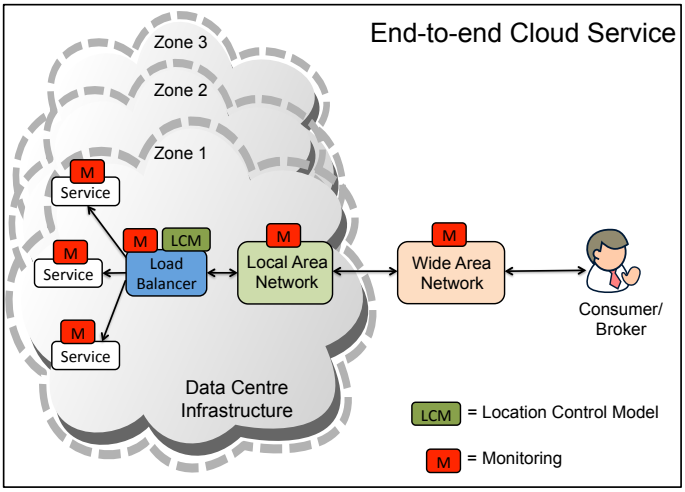


Figure 5. Cloud Service Provisioning Use Case Scenario

Based on this use case scenario, we demonstrate our approach, which is aimed at increasing assurance to consumers through continuous communication of trustworthiness information. For this demonstration, we deploy an online web-shop and image rendering application on the OpenStack Cloud platform to represent the consumer service. The consumer offers this service to its users based on Service Level Agreements (SLA), which stipulates penalties in case of poor service performance.

1939-1374 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2016.2553036, IEEE Transactions on Services Computing

To support the consumer in guaranteeing the agreed SLA with his/her users, we employ the Service Monitor Framework, which consists of different monitoring tools that are capable of monitoring each of the components involved in the Cloud service provisioning as shown in Figure 5. The monitored data provide the required insight for consumers to increase their assurance perception and dependability on Cloud services.

Furthermore in Figure 5, we present the data location control model, which controls the location of consumer data. This component is deployed in parallel to the load balancer as shown in Figure 5. It is responsible for controlling the consumer data location among the Cloud data centre zones.

In the following, we demonstrate how we communicated trust information to the Cloud consumer (broker) by detailing the monitoring strategy of each quality assurance metric.

5.2.1 Data Location

To evaluate the data location, we created sub-networks in our OpenStack Cloud platform to represent different zones and we deployed the location control model to manage data movements between the zones. Each zone is identified by distinct IP ranges used in configuring the virtual machines. This control model informs the consumer whenever his/her service application data changes location through the data location metric. In this evaluation, the value of the data location metric is demonstrated on the trust label interface as shown in Figure 6. This metric is clickable to provide detailed information about the data location.

5.2.2 Service Uptime

The service uptime metric on the trust label interface represents the percentage of time when a particular service is available to customers. It is an important metric in the management of service provisioning to supervise availability. To monitor the service uptime status, the Service Monitor Framework includes a monitoring tool that uses HTTP ping to measure uptime. The HTTP technologies are used to enable interoperability among diverse Cloud services in our approach.

To observe the service uptime and communicate trustworthiness information to the consumer, we use the monitoring tool to supervise the consumer web application by periodically sending a HTTP request to it and checking the status code of the response. The resulting data is communicated to the consumer through the trust label interface and also inserted into a database for calculating the running average metrics. Figure 6 shows the service uptime monitored results.

5.2.3 Internal Network Uptime

The internal network uptime metric shows the percentage of time during which the local network in a Cloud data centre infrastructure is up and running as shown in Figure 5.

This metric ensures that the consumer web application service is working properly within the Cloud platform, for example, to check if the internal connectivity to the database server is up. To monitor this metric and send status information to the consumer, the Service Monitor Framework includes a tool that uses network pinging to watch the local area network. This is done by sending multiple pings between the virtual machines and checking their responses. These multiple pings enable testing of different aspects of the local area network to ascertain that they are up and running. It also increases the validity of the achieved results since a virtual machine could be down and unreachable while the local area network is up. The resulting monitoring data is communicated to the consumer through the trust label interface shown in Figure 6.

Cloud Solutions

Dummy CRMA
New York, NY10006
State of New York, USA

		Performance	Policy	Preference
		Can I measure ?	Is there a policy ?	Can I modify ?
Data Security		YES	YES	YES
Certification		YES	YES	YES
Service Levels		YES	YES	YES
Variation of Terms		YES	YES	YES
Data Portability	Onboard	YES	YES	YES
	Offboard	YES	YES	YES
Backup of Data		YES	YES	YES
Data Location		YES	YES	YES
Ownership	Data	N/A	YES	YES
	Meta Data		YES	YES
	Service Customisation		YES	YES
	Application Customisation		YES	YES
Sharing of Data	Commercial	NO	YES	YES
	Legal	NO	YES	YES
Insurance Levels		YES	YES	YES
Audit Approvals		YES	YES	YES
Customer Service Level		YES	YES	YES

Service Level Summary

	Target	Current	3-Month	12-Month
Service Uptime	100%	100%	100%	99.99%
Internal Network Uptime	100%	100%	100%	99.999%
External Network Uptime	100%	100%	100%	100%
Dynamic Load Balancing	100%	100%	100%	100%
Cloud Storage Service	100%	100%	99.99%	99.999%
Primary DNS Availability	100%	100%	100%	100%
Server Reboot	<15m	0.00045mins	0.00045mins	0.00045mins
Emergency Support Response Time	<30m	10mins	14.5mins	15.2mins
General Support Response Time	<120m	35mins	40mins	45mins
Engineering Support	23 x 365	Yes	N/A	N/A
Physical Security	24 x 365	Yes	N/A	N/A

Figure 6. Trust Label Interface Displaying Evaluation Results

5.2.4 External network Uptime

The external network uptime metric represents the percentage of time during which the wide area network connecting a Cloud data centre infrastructure and a consumer is available. Figure 5 shows the position of the wide area network in the end-to-end Cloud service provisioning setup.

This metric informs the consumer about the network accessibility of the deployed web application service by his/her users. To observe and communicate the status information of this metric to the consumer, the Service Monitor Framework includes a tool that continuously queries

1939-1374 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2016.2553036, IEEE Transactions on Services Computing

the availability of this metric. This tool queries different public domains from both the Cloud data centre machines and a machine outside the OpenStack platform acting as an external side. The response data from both sides are processed and compared for correctness before informing the consumer about the status of the metric through the trust label interface as shown in Figure 6. The double check is carried out to avoid false results in cases where the Cloud data centre might not be able to reach the external network due to some internal network issues.

5.2.5 Dynamic Load Balancing

This metric represents the availability of the dynamic load balancer. It is expressed as a percentage. The load balancer is responsible for balancing service requests among the computing resources on a Cloud platform. Load balancing in Clouds can be achieved with a dedicated software or hardware device. Therefore, to accommodate the monitoring of these varieties, we developed two tools in the Service Monitor Framework - one based on HTTP queries and the other based on network pinging. The HTTP queries are used to monitor the software load balancer while the network pinging is used to monitor hardware load balancers such as multilayer switches.

Our evaluation testbed includes a software load balancer. Hence, to monitor this component and communicate performance and status information to the consumer, we employ the HTTP query tool to continuously query this component and process the response data, which indicate whether it is functioning or not. This information is sent to the consumer through the trust label interface as shown in Figure 6. The monitoring data is also being stored in a database for calculating the historical averages.

5.2.6 Cloud Storage Service

The Cloud storage service defines a metric for monitoring the availability of Cloud provisioned storages. This metric shows in percentage, the duration of time during which a Cloud storage service is available. A Cloud storage service typically refers to a hosted object storage service. However more recently, the scope has been broadened to include other storage types like block storage. In the Service Monitor Framework, we implemented two tools for monitoring the availability of object and block storages.

The consumer web application service in this use case scenario uses object storage to store user rendered video files on the OpenStack Cloud platform. To observe the availability of this service and timely inform the consumer, the monitoring framework periodically writes and reads a file to and from the storage container. An unsuccessful write to the object storage, or an unsuccessful read from it, could mean unavailability of the service. However, we take the background network status into consideration because a network failure could lead to an unsuccessful write or read while the object storage is up and running. The achieved results are transparently communicated to the consumer through the trust label interface as shown in Figure 6 and as well stored in a database for historical average calculations.

5.2.7 Primary DNS Availability

This metric presents the availability status of the primary Domain Name Service (DNS). The unit of this metric values is in percentage. The primary DNS is responsible for translating human-friendly domain names into Internet Protocol (IP) addresses and vice versa. There is usually a secondary DNS, which combines with the primary one to provide high availability and redundancy. A monitoring tool was developed in the Service Monitor Framework for measuring this metric.

The DNS server translates the Unified Resource Locator (URL) that points to the consumer web application service into IP for internal communication. This enables users to reach and use the service through a URL. To monitor the DNS server availability in order to inform the consumer of its status, we deploy an agent on a separate machine on the OpenStack Cloud platform that continuously sends translate requests at a given interval to this server. The response data were analysed to determine if the server was responding and also correctly translating the domain names. The resulting data are communicated to the consumer through the trust label interface as shown in Figure 6 as well as persisted in a database for historical average calculations.

5.2.8 Server Reboot

The server reboot metric measures the time it takes to reboot a virtual machine in a Cloud environment. Monitoring of this metric enables many important resource management and energy efficiency strategies such as on-demand provisioning. When the duration of time it takes to startup a new machine is known, one could then easily manage the starting and stopping of machines to accommodate peak times. The Service Monitor Framework implements a tool for observing this metric. This tool is capable of monitoring the boot/reboot time of local and remote machines.

This metric informs the consumer the length of time it would take for the web application service to be available after a system reboot. We monitor this metric by measuring the length of time it takes for shutting down and starting different virtual machines deployed on the OpenStack Cloud platform. The resulting boot time information is communicated to the consumer through the trust label interface as shown in Figure 6 as well as stored in a database for calculating historical averages.

5.2.9 Other Metrics

The remaining four metrics in this section are not dynamically monitored because the first two metrics are dependent on internal customer support system, like phone, email, chat, and the last two metrics are not measurable at runtime. The following explains the metrics:

- **Emergency Support Response Time:** This metric describes the length of time it takes a Cloud provider to respond to an emergency situation arising from service provisioning.
- **General Support Response Time:** This metric describes the amount of time it takes a Cloud provider to address customer issues regarding service usages and provide support.

1939-1374 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2016.2553036, IEEE Transactions on Services Computing

- **Engineering Support:** This metric informs if a service provider offers engineering supports to potential customers for integrating or adapting their services.
- **Physical Security:** It shows if there are physical security measures in a Cloud provider data centre infrastructure.

The values of these metrics are manually monitored and communicated in an appropriate format to the consumer through the trust label interface.

5.3 Use Case Result Summary

The achieved results are presented in a snapshot of the trust label interface as shown in Figure 6. This figure demonstrates the operationalisation and the transparent communication of trustworthiness information to Cloud consumers using the trust label system. The focus of this operationalisation effort is on data location and the measurable metrics. This is because the data location metric represents an important factor in raising a provider's trustworthiness since consumers are sensitive regarding where their data are being kept. The supervision of the data location metric in this use case scenario has demonstrated the consumer how his/her data is being handled. It has provided the ability to control and manage data movements in a Cloud environment to the consumer. This gives consumers a sense of transparency and control, and thereby increases their trust in, and dependability on, Cloud services.

The service level summary section of the trust label interface, as shown in Figure 6, presented the observable metrics. Note that not all the metrics in that section are dynamically monitored at run-time as explained previously. The monitored values of these metrics are being continuously used to update the trust label interface in order to inform the consumer about their current status. They are as well stored in a database for historical reasons.

Based on the monitored historical data stored in the database, the "3-Month" and "12-Month" average values are recalculated. We did not run the evaluations for over twelve months to calculate these values. Instead we used a shorter interval of hours to simulate them for this evaluation. However, on our production server where the trust label system is deployed, it is configured to be calculated at three and twelve months intervals.

The trust label interface presented in Figure 6 is a snapshot taken at run-time during the evaluations. This snapshot is presented as proof of concept since the entire interface is large and repeating it multiple times to show value changes is beyond the scope and length of this paper. The trust label focuses on Cloud Service Providers (CSP) and specific service they offer e.g., if a CSP has multiple services, you would need multiple labels. However, this use case demonstration is for a service only and can be a prior and post factor from a contractual perspective. As such it both addresses the calculus based trust through the service level summary and access to performance data and knowledge based trust through predictability and transparency (knowledge sharing).

5.4 Discussion

Establishing and maintaining consumer trust are key factors in achieving success as a Cloud provider. The Cloud marketplace contains a multitude of providers offering seemingly similar services. A lack of transparency around their operations prevents consumers from making informed choices regarding which services and providers are more trustworthy than others. This has created a situation where it is very difficult for consumers to build knowledge based trust on their providers. This is impacting the rate of adoption and usage of Cloud technologies. We presented a practical use case scenario in our evaluations to demonstrate the provisioning of a consumer Cloud services that resells them to his/her users. We highlighted the factors that could inhibit consumer trust and dependence on Cloud services.

The evaluation of the trust label system using the described use case scenario provides consumers with reliable real-time information about the quality of their Cloud services in a clear and transparent manner. The label was designed building on the work of Kelley *et al.* [47], and the well-established nutritional label featured on food packaging. In our evaluations, we demonstrated how specific aspects of that label can be operationalised. Although previous authors have suggested that online trust can be built through the use of trust and assurance seals, the impact of these trust seals has been somewhat mixed [48].

The trust label presented here goes further than traditional trust marks and seals in providing actual real time information about the performance and policies of Cloud services. Unlike previous attempts at engendering trust including trust marks and digital seals, which are static, the proposed trust label interface provides detailed information that is continually updated to show the performance of Cloud services. This is essential given the complexity and continuous change in the Cloud environment where consumers need up-to-date information to make informed trust decisions.

The operationalisation efforts and the use case demonstration presented in this paper represent a major step towards the launch of a fully functional and dynamic trust label system. Based on such system, Cloud providers could easily introduce new functionalities. However, in its current state, further work is still necessary to implement the contract condition composite metric group. In addition, the use case evaluations demonstrated the technical realisation and operations of the trust label system in communicating information. It is limited in terms of showing the actual user trust perception. Empirical evaluations of user experiences will be necessary to complement our current effort and to fully show the potentials of the trust label system on increasing the consumer trust.

6 Conclusion

In this paper, we presented a trust label system, its technical realisation and the operationalisation of the complete system. The system was designed for communicating trustworthiness to Cloud consumers.

We described the trust label components and focused on two groups of composite metrics: execution and data

1939-1374 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2016.2553036, IEEE Transactions on Services Computing

management metrics. To demonstrate the data management metric group operationalisation, a data location control model was designed to grant consumers the ability to specify locations in a policy where they wish to store their data. The policy is transparently enforced by allowing consumers to view the location of their data, and also to inform them in case of any change. The execution metric group was operationalised by monitoring the service level metrics using a service monitor framework. This framework is designed to compose diverse monitoring tools that can be executed in parallel to monitor different metrics and to communicate the monitored data to the trust label interface.

For the evaluation of the system, a practical use case scenario was introduced. This use case describes an end-to-end consumer service provisioning in Clouds. It explains clearly how the quality of service elements of the deployed Cloud services were monitored and communicated to the consumer through the trust label interface. The monitored values are stored as well in a database to enable the calculation of the average historical "3-Month" and "12-Month" data. A snapshot of the trust label interface was presented to show the results achieved.

In summary, our core objective in this paper is to operationalise the Cloud trust label system. In doing so, we move closer to developing a system that provides transparency and insight for consumers into Cloud service provisioning operations in order to communicate trustworthiness. The proposed trust label represents a significant improvement on previous approaches by allowing Cloud service providers to communicate detailed and up-to-date information to their consumers. This information will allow consumers to make meaningful comparisons across providers and to build perceptions of knowledge based trust.

In a future work, we intend to integrate the trust label system with CSA CloudTrust protocol to support security metrics, and to conduct experiment studies with end-users to gather empirical evidence about the effects of the trust label system on their trust in Cloud services and providers. This will provide further validation of the potential impact of the trust label and help to improve the design of the operationalised trust label system by identifying metrics that are considered most important by end users. In addition, future experiments will inform on the novelty of the system from the users perspective. We aim to publish the entire system under an open source license to broaden its usage and thereby support our vision of increasing Cloud service adoption by consumers.

ACKNOWLEDGMENTS

The research work described in this paper was supported by the Irish Centre for Cloud Computing and Commerce, an Irish national Technology Centre funded by Enterprise Ireland and the Irish Industrial Development Authority.

REFERENCES

[1] Gartner, "Gartner predicts special report," 2015, http://www.gartner.com [Retrieved: 7-05-2015].
[2] S. Reid and H. Kilster, "Sizing the cloud," 2011, forrester Research Report.
[3] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing - the business perspective," *Decision Support Systems*, vol. 51, no. 1, pp. 176 – 189, 2011.
[4] European Commission, "Potential and impacts of cloud computing services and social network websites," 2014, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513546/IPOL-JOIN_ET(2014)513546_EN.pdf [Retrieved: 17-04-2015].
[5] Bradshaw, David, et al., "Quantitative estimates of the demand for cloud computing in europe and the likely barriers to uptake," 2012, SMART2011/0045.
[6] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," *Internet Computing, IEEE*, vol. 14, no. 5, pp. 14–22, Sept 2010.
[7] T. Lynn, L. van der Werff, G. Hunt, and P. Healy, "A delphi approach to the development of a cloud trust label," *Journal of Computer Information Systems*, vol. in press, 2015.
[8] M. Söllner, P. Pavlou, and J. M. Leimeister, "Understanding trust in it artifacts a new conceptual approach," in *Academy of Management Annual Meeting*, Orlando, Florida, USA, 2013.
[9] P. A. Pavlou and A. Dimoka, "The nature and role of feedback text comments in online marketplaces: Implications for trust building, price premiums, and seller differentiation," *Journal of Information System Research*, vol. 17, no. 4, pp. 392–414, Dec. 2006.
[10] W. Wang and I. Benbasat, "Attributions of trust in decision support technologies: A study of recommendation agents for e-commerce," *Journal of Management Information System*, vol. 24, no. 4, pp. 249–273, April 2008.
[11] N. G. Carr, "The end of corporate computing," *MIT Sloan Management Review*, vol. 46, no. 3, pp. 67– 73, 2005.
[12] P. A. Pavlou, "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model," *International Journal of Electronic Commerce*, vol. 7, no. 3, pp. 101–134, Apr. 2003.
[13] A. Beldad, M. de Jong, and M. Steehouder, "How shall i trust the faceless and the intangible? a literature review on the antecedents on municipal websites," *Government Information Quarterly*, vol. 27, no. 3, pp. 238–244, 2010.
[14] J. Boyd, "The rhetorical construction of trust online," *Communication Theory*, vol. 13, no. 4, pp. 392–410, 2003.
[15] S. Shek, C.-L. Sia, and K. Lim, "A preliminary assessment of different trust formation models: the effect of third party endorsements on online shopping," in *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on*, Jan 2003, pp. 10 pp.–.
[16] D. M. Rousseau and S. B. Sitkin, "Introduction to special topic forum. not so different after all: A cross-discipline view of trust," *Academy of Management Review*, vol. 23, no. 3, pp. 393–404, 1998.
[17] P. Ping Li, "When trust matters the most: The imperatives for contextualising trust research," *Journal of Trust Research*, vol. 2, no. 2, pp. 101–106, 2012.
[18] M. Söllner, A. Hoffmann, and J. M. Leimeister, "Why different trust relationships matter for information systems users," *European Journal of Information Systems*, pp. 1 –14, 2015.
[19] K. T. Dirks and D. L. Ferrin, "Trust in leadership: meta-analytic findings and implications for research and practice," *Journal of applied psychology*, vol. 84, no. 4, p. 611, 2002.
[20] R. J. Lewicki and B. B. Bunker, "Developing and maintaining trust in work relationships," in *Trust in organizations: Frontiers of theory and research*, R. M. Kramer and T. R. Tyler, Eds. Sage Publications, 1996, pp. 114 – 139.
[21] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *The Academy of Management Review*, vol. 20, no. 3, pp. 709–734, 1995.
[22] D. H. Mcknight, M. Carter, J. B. Thatcher, and P. F. Clay, "Trust in a specific technology: An investigation of its components and measures," *ACM Transactions on Management Information System*, vol. 2, no. 2, Jul. 2011.
[23] G. Dietz, "Partnership and the development of trust in british workplaces," *JHuman resource Management Journal*, vol. 14, no. 1, pp. 5 – 24, 2004.
[24] K. Aiken and D. Boush, "Trustmarks, objective-source ratings, and implied investments in advertising: Investigating online trust and the context-specific nature of internet signals," *Journal of the Academy of Marketing Science*, vol. 34, no. 3, pp. 308–323, 2006.
[25] D. Aiken, G. Osland, B. Liu, and R. Mackoy, "Developing internet consumer trust: Explaining trustmarks as third-party signals," in *AMA Winters Educators Conference Proceedings*, 2006.

1939-1374 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2016.2553036, IEEE Transactions on Services Computing

[26] L. Remotti, "Presentation at eu digital agenda assembly," in *Trustmark Provision in Europe*, 2012.

[27] I. Somerville, "Design for failure: Software challenges of digital ecosystems," in *Digital EcoSystems and Technologies Conference, 2007. DEST '07. Inaugural IEEE-IES*, Feb 2007, p. 1.

[28] J. Kim and J. Y. Moon, "Designing towards emotional usability in customer interfaces - trustworthiness of cyber-banking system interfaces," *Interacting with Computers*, vol. 10, no. 1, pp. 1 – 29, 1998, {HCI} and Information Retrieval.

[29] Y. Bart, V. Shankar, F. Sultan, and G. L. Urban, "Are the drivers and role of online trust the same for all web sites and consumers? a large-scale exploratory empirical study," *Journal of Marketing*, vol. 69, no. 4, pp. 133–152, 2005.

[30] M. Koufaris and W. Hampton-Sosa, "The development of initial trust in an online company by new customers," *Information & Management*, vol. 41, no. 3, pp. 377 – 397, 2004.

[31] P. A. Pavlou and D. Gefen, "Building effective online marketplaces with institution-based trust," *Journal of Information System Research*, vol. 15, no. 1, pp. 37–59, Mar. 2004.

[32] I. Benbasat and W. Wang, "Trust in and adoption of online recommendation agents," *Journal of the Association for Information Systems*, vol. 6, no. 3, p. 4, 2005.

[33] H. Hoffmann and M. Söllner, "Incorporating behavioral trust theory into system development for ubiquitous applications," *Personal Ubiquitous Computing*, vol. 18, no. 1, pp. 117–128, 2014.

[34] X. Hu, G. Wu, Y. Wu, and H. Zhang, "The effects of web assurance seals on consumers' initial trust in an online vendor: A functional perspective," *Decision Support Systems*, vol. 48, no. 2, pp. 407 – 418, 2010.

[35] K. Özpolat and W. Jank, "Getting the most out of third party trust seals: An empirical analysis," *Decision Support Systems*, vol. 73, no. 0, pp. 47 – 56, 2015.

[36] D. Cyr, M. Head, and H. Larios, "Colour appeal in website design within and across cultures: A multi-method evaluation," *International Journal of Human-Computer Studies*, vol. 68, no. 1-2, pp. 1–21, Jan. 2010.

[37] A. N. Tuch, J. A. Bargas-Avila, and K. Opwis, "Symmetry and aesthetics in website design: It's a man's business," *Journal of Computers in Human Behavior*, vol. 26, no. 6, pp. 1831–1837, Nov. 2010.

[38] M. M. Head and K. Hassanein, "Trust in e-Commerce: Evaluating the Impact of Third-Party Seals," *Quarterly Journal of Electronic Commerce*, vol. 3, no. 3, pp. 307–325, 2002.

[39] D. H. McKnight, C. J. Kacmar, and V. Choudhury, "Dispositional trust and distrust distinctions in predicting high- and low-risk internet expert advice site perceptions," *e-Service Journal*, vol. 3, no. 2, pp. pp. 35–58, 2004.

[40] T. Lynn, P. Healy, R. McClatchey, J. Morrison, C. Pahl, and B. Lee, "The case for cloud service trustmarks and assurance-as-a-service," in *International Conference on Cloud Computing and Services Science Closer'13*, 2013.

[41] R. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "Trustcloud: A framework for accountability and trust in cloud computing," in *Services (SERVICES), 2011 IEEE World Congress on*, July 2011, pp. 584–588.

[42] H. A. Linstone and M. Turoff, "The delphi method," in *Reading, MA: Addison-Wesley*, 1975, pp. 3 – 12.

[43] K. Fatema, P. Healy, V. C. Emeakaroha, J. P. Morrison, and T. Lynn, "A user data location control model for cloud services," in *International Conference on Cloud Computing and Services Science, CLOSER 2014*, 2014, pp. 476–488.

[44] V. C. Emeakaroha, I. Brandic, M. Maurer, and S. Dustdar, "Low level metrics to high level slas - lom2his framework: Bridging the gap between monitored metrics and sla parameters in cloud environments," in *2010 International Conference on High Performance Computing and Simulation (HPCS)*, July 2010, pp. 48 –54.

[45] K. Fatema, V. C. Emeakaroha, P. D. Healy, J. P. Morrison, and T. Lynn, "A survey of cloud monitoring tools: Taxanomy, capabilities and objectives," *Journal of Parallel and Distributed Computing*, vol. 74, pp. 2918–2933, 2014.

[46] A. Videla and J. J. Williams, *RabbitMQ in Action: Distributed Messaging for Everyone*. Manning Publications Company, 2012.

[47] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, "A "nutrition label" for privacy," in *Proceedings of the 5th Symposium on Usable Privacy and Security*, ser. SOUPS '09. New York, NY, USA: ACM, 2009, pp. 4:1–4:12.

[48] D. P. Cook and W. Luo, "The role of third-party seals in building trust online," *e-Service Journal*, vol. 2, no. 3, pp. pp. 71–84, 2003.

1939-1374 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2016.2553036, IEEE Transactions on Services Computing

BIBLIOGRAPHY



Dr. Vincent C Emeakaroha is a postdoctoral researcher at the Irish Centre for Cloud Computing and Commerce affiliated with University College Cork. He has over 6 years experience in Cloud monitoring and service provisioning management. He received bachelor degree in Computer Engineering in 2006 and acquired double masters in Software Engineering & Internet Computing in 2008 and in Computer Science Management in 2009. In 2012, he received his Ph.D in Computer Science all from Vienna University of Technology. His research areas of interest include Cloud computing, autonomic computing, energy efficiency in Cloud, SLA and QoS management.



Dr. Kaniz Fatema is working as a Research Fellow at ADAPT centre of Trinity College Dublin. Previously she worked at Irish Centre for Cloud Computing and Commerce of University College Cork as a post-doctoral researcher. Her Ph.D. research was conducted under EC FP7 project (Trusted Architecture for Securely Shared Services) at the University of Kent, UK. She obtained her M.Sc. (Eng) in Data Communications from the University of Sheffield, UK with distinction. She did M.Sc. and B.Sc. (honors) in Computer Science and Engineering from the University of Dhaka, Bangladesh. She worked as a Lecturer at Stamford University Bangladesh for 2 years and as an Assistant Lecturer at the University of Kent, UK for 3.5 years.



Dr. Lisa van der Werff is an organisational psychologist and postdoctoral researcher with the Irish Centre for Cloud Computing and Commerce. Her research interests are in the area of trust decision making, maintenance and repair. Lisa also has an interest in quantitative research methodologies including structural equation modelling, latent growth modelling, Bayesian analysis and big data analysis. Her research with IC4 focuses on how Cloud service providers can communicate trustworthiness to consumers and on trust repair processes following data breach. Lisa holds a PhD and MSc in Work and Organisational Psychology from DCU Business School as well as a BA in Psychology from NUI Maynooth. Her PhD was completed with support from the Daniel OHare Scholarship Fund as part of the National Development Plan. During her PhD, Lisa spent a semester as a visiting scholar in the University of Georgia, USA. Lisa also has over 6 years of industry experience working as a learning and development specialist and human resources professional for KPMG and McCann FitzGerald Solicitors.



Dr. Philip Healy has over a decades experience in parallel and distributed software development, in both academic and industrial settings. His recent academic work includes the research and development of a remote monitoring system for physiological signals acquired in a critical care setting. His recent industry experience includes the design and development of large-scale distributed data processing applications using cutting-edge technologies such as Hadoop and HBase. He is currently a Research Fellow at The Irish Centre for Cloud Computing & Commerce.



Prof. Theo Lynn is the Business Innovation Platform Director at Dublin City University and a Senior Lecturer at DCU Business School. He is founder and Principal Investigator at the Irish Centre for Cloud Computing and Commerce, an Enterprise Ireland/IDA funded industry-led research centre located at Dublin City University.



Prof. John P Morrison is the founder and director of the Centre for Unified Computing. He is a co-founder and co-director of the Boole Centre for Research in Informatics and a co-founder and co-director of Grid-Ireland. He is the UCC PI for the Irish Centre for Cloud Computing and Commerce. Prof. Morrison is a Science Foundation of Ireland Investigator award holder and has published widely in the field of Parallel Distributed and Grid Computing. He has been the guest editor on many journals including the Journal of Super Computing and the Journal of Scientific Computing. He is on the Editorial Board of Multi-Agent and Grid Systems: An International Journal, published by ISO Press, and the International Journal of Computational Intelligence: Theory and Practice (IJCITP). He is a member of the ACM and a senior member of the IEEE. Prof Morrison is a member of the I2Lab Advisory Board in the University of Central Florida.

1939-1374 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.