

RESEARCH

Open Access



Modelling trust and risk for cloud services

Erdal Cayirci^{1*} and Anderson Santana de Oliveira²

Abstract

A joint trust and risk model is introduced for federated cloud services. The model is based on cloud service providers' performance history. It addresses provider and consumer concerns by relying on trusted third parties to collect soft and hard trust data elements, allowing for continuous risk monitoring in the cloud. The negative and positive tendencies in performance are differentiated and the freshness of the historic data is considered in the model. It addresses aleatory uncertainty through probability distributions and static stochastic simulation. An analytical insight into the model is also provided through the numerical analysis by Monte-Carlo simulation.

Keywords: Cloud computing, Accountability, Risk, Trust, Reputation, Risk model, Risk assessment, Service mashup, Inter-cloud, Cloud federation

Background

New cloud services and architectures are introduced every day, and cloud service providers (CSP) begin federating cloud services as cloud service mashups [3, 7–10, 22–24, 55]. A cloud service mashup (CSM) comprises multiple cloud services of various delivery models (i.e., IaaS, PaaS or SaaS) for providing a composite service, and can be in one of the following structures:

- Intra data-center: All the cloud services in the fan-in of a CSM (i.e., the services that compose the CSM) are co-located in the same data center.
- Inter data-centre: The cloud services in the fan-in of a CSM are located in multiple data centres owned by the same CSP.
- Inter cloud service provider: The cloud services in the fan-in of a CSM are located in multiple data centres owned by multiple CSPs.

We call intra data-centre and inter data-centre mashups as internal and inter CSP mashups as external CSM.

The outsourcing model of CSM presents economic and technological advantages. However, it also impacts on data governance, as risks and compliance management are delegated to third parties. The security practices of these

third parties may not be visible to cloud customers (CCs), raising the question about the accountability of service providers when processing data in highly dynamic and heterogeneous environments. Accountability regards the data stewardship regime in which organisations that are entrusted with personal and business confidential data are responsible and liable for processing, sharing, storing and using the data according to the contractual and legal constraints from the time it is collected until when the data is destroyed [47].

CCs need to trust that their CSP secure the CC data, and to provide the quality of service (QoS) and grade of service (GoS), i.e., service level objectives (SLO) agreed in service level agreements (SLA). Hence, both CC and CSP take risk. The risk taken by CCs is that their operations may be hampered due to service outages, security or privacy breaches. The risk for CSPs is two folded: They may not be able to fulfil SLOs agreed in an SLA, and therefore face penalties and loose reputation. Secondly, a CSP may also be a CC for the services provided by the other clouds in a CSM, and therefore CSPs are also subject to the risks similar to the ones taken by CCs.

There are various models developed to analyse and to assess the risks and the trustworthiness of information systems and services. We provide a short survey on them in Section “[Related work and definitions](#)”. To the best of our knowledge, there is not a quantitative risk and trust model which is based on the CSP performance data and can be used for internal and external CSM. In

* Correspondence: erdal.cayirci@uis.no

¹Electrical Engineering and Computer Science Department, University of Stavanger, Stavanger, Norway

Full list of author information is available at the end of the article

this paper, we introduce a new quantitative and stochastic scheme called joint risk and trust model (JRTM) for CSMs. JRTM is based on the definitions made by “Accountability for Cloud and Other Future Internet Services” (A4Cloud), which was a large European Union Framework Seven Project with partners from academia (i.e., law, data science and computer science departments) and industry. A4Cloud contacted with many stakeholders including users and organizations, such as, Cloud Security Alliance to determine and to verify the risk and trust parameters and their inter-relations. JRTM is a product of the A4Cloud Project and provides a quantitative scale to analyse the risk and trust jointly.

JRTM is based on a stochastic process, and therefore addresses uncertainty. It uses observations that we call evidence to assess the risk and to build trust for a CSP. These observations are in abstract level such that the details about threats, vulnerabilities, CSP architectures and security schemes are not needed for the risk assessment. Hence, JRTM is low cost, scalable and practical. JRTM depends on historic data collected by a trust as a service (TaaS) provider, a trusted third party, who makes recommendations about the trustworthiness of a CSM. TaaS approach helps overcoming barriers due to the lack of transparency. The level of risks acceptable for a CSM is defined by the TaaS Provider and CC together. CC also provides several parameters that influence the effects of the historic data to the results of the model based on the freshness and the tendency of the data (i.e., if it changes in negative or positive direction).

Both risk and trust have been extensively studied in various contexts for hundreds of years. Risk management, and specifically risk assessment for IT has also been a hot research topic for several decades [25, 32]. On the other hand, modelling risk and trust for cloud computing and associating it with the notion of accountability has attracted researchers only recently [29, 46]. In Section “[Related work and definitions](#)”, we provide a short survey on these recent risk and trust modelling related work. In the same section, we also give some definitions for the terms that we refer later. We explain the details about our new model, JRTM, in Section “[Joint trust and risk model for cloud service mashups](#)”. We analyse the sensitivity of JRTM against several engineering parameters by using the results from our simulation based experiments in Section “[Experimental results](#)”. The performance of JRTM is also evaluated in the same section. Finally, we conclude our paper in Section “[Conclusions](#)”.

Related work and definitions

International Organization for Standardization (ISO) published a standard on Risk Management [27], ISO 31000,

and the joint publication by ISO and The International Electrotechnical Commission (IEC) complemented ISO 31000 with the publication of ISO/IEC 31010 [19, 28] about risk assessment techniques. Both of these standards are generic. Information Technology (IT) Governance Institute and the Information Systems Audit and Control Association (ISACA) introduced COBIT in 1996, which is a common language to communicate the goals, objectives and results of businesses. The latest version of COBIT is from 2013 and provides recommendations also on enterprise risk management [26]. COBIT is a generic framework for information technology (IT), and its adaptation to Cloud Computing has been made for selected cases [21]. JRTM is a quantitative risk assessment scheme specifically designed for cloud service mashups and complies with the definitions made in all of these standards.

In its recommendations on risk assessment for cloud computing [18], European Network and Information Security Agency (ENISA) provides a list of relevant incident scenarios, assets and vulnerabilities. It suggests estimating the level of risk on the basis of likelihood of a risk scenario mapped against the estimated negative impact, which is the common approach for the risk formulation in the literature [4, 11, 12, 27, 28, 32]. Although ENISA’s recommendations are specific for cloud approach, it is a generic framework that does not provide a way to map the specifics of CSPs and CCs to the 35 risk scenarios listed in the report [18]. This risk assessment by ENISA is based on a qualitative inductive risk model. Another qualitative inductive scheme is by “The Commission nationale de l’informatique et des libertés” (CNIL), in English “*The French National Commission on Informatics and Liberty*” [12] more recently. CNIL’s methodology is similar to the one by ENISA with the following differences: It is a risk assessment focused on privacy risks in cloud computing. It also recommends measures to reduce the risks and assess the residual privacy risks after the application of these measures. However, it is still generic and does not differentiate CSPs or CCs. JRTM is also a risk assessment scheme similar to ENISA’s assessment and CNIL’s report. However, it is not generic for cloud approach as ENISA and CNIL methodologies but for a specific cloud service mashup and a CC. Another difference is that JRTM is dynamic (i.e., not a fixed risk assessment for cloud concept), quantitative and based on historic data.

Cloud Security Alliance Cloud Assessment Initiative Questionnaire (CAIQ) [13] is a questionnaire prepared for CSPs to document the implemented security measures. It is based on the Cloud Control Matrix (CCM) taxonomy of security controls. The questionnaire has been answered by many CSPs, and is publicly available

in CSA Security, Trust and Assurance Registry (STAR) [15]. Cloud Adoption Risk Assessment Model (CARAM) [11] is a model developed and implemented by A4Cloud recently. CARAM is another qualitative model that adapts the methodology and assessments made by ENISA and CNIL to assess the risk for a given CSP-CC pair. It is a decision support tool designed to help CCs in selecting a CSP that fits best to their risk profile. It is different from JRTM because it is a qualitative scheme, and it does not use performance data related to CSPs but the information about how CSPs implement the security measures.

A risk is the product of a threat, a vulnerability and the consequences (i.e., the impact of an incident) [17, 20, 32], and cloud computing is subject to a long list of threats [14] and vulnerabilities [9]. A CC has a special challenge in risk assessment for the cloud when compared to conventional information technology (i.e., other than cloud) customers. CSPs usually keep the locations, architecture and details about the security of their server farms and data centers confidential from CCs. Therefore, it is more difficult to a CC to assess all the threats and vulnerabilities. Additionally, CSPs have to prioritize the issues to solve when risks are realized. A CC has to rely on the autonomic procedures of CSP for managing the infrastructure appropriately according to the CCs' security dynamics, treating the CCs' issues in a timely manner, detecting, recovering and reporting the security incidents accurately. These uncertainties increase risk and imply that the CCs have to trust CSP [50], and on its certifications, without further insight into the real time risk landscape. JRTM takes all these facts into account. For risk assessment, JRTM does not require the details about the technical structure, vulnerabilities and threats specific to a CSP.

Risk and trust should not be treated as related only to security but also QoS and GoS. The centralization and mutualization of resources reduce the costs. However, shared resources may be congested from time to time. Congestion control, service differentiation, user differentiation and prioritization are complex challenges especially for large clouds with high scalability requirements. The CCs need to be assured that their SLOs on GoS and QoS requirements are fulfilled and their operations are not hampered due to congested cloud resources. Providing such an assurance, measuring and guaranteeing QoS/GoS are not trivial tasks. JRTM treats QoS and GoS related risks within the service risk domain based on the SLOs agreed in SLAs.

Accountability [46] and trust are concepts required to be realized before potential CCs embrace cloud computing approach. Therefore, "trust" with cloud computing perspective has attracted researchers recently [45, 49],

and "trust as a service" is introduced to the cloud business model. Standardised trust models are needed for verification and assurance of accountability, but none of the large number of existing trust models to date is adequate for the cloud environment [34]. There are many trust models which strive to accommodate some of the factors defined by [35] and others [6] and there are many trust assessment mechanisms which aim to measure them.

Definition of trust can be a starting point for modeling it. In [39, 50], trust is defined as "the willingness of a party to be vulnerable to the action of another party based on the expectation that the other will perform a particular action important to the trusting party, irrespective to the ability to monitor or control the trusted party". This definition does not fully capture all the dynamics of trust, such as the probabilities that the trustee will perform a particular action and will not engage in opportunistic behavior [45]. There are also hard and soft aspects of trust [42, 53, 60]. Hard part of trust depends on the security measures, such as authentication and encryption, and soft trust is based on things like brand loyalty and reputation. In [51], the authors introduce not only security but also accountability and auditability as elements which impact CC trust in cloud computing and show that they can be listed among the hard aspects. In [31], SLA is identified as the only way that the accountability and auditability of a CSP is clarified and therefore a CSP can make CCs trust them. The conclusion is that "trust" is a complex notion to define. Although JRTM is a quantitative model, it differentiates the soft and hard parts of the trust. To the best of our knowledge, JRTM is the only model specifically designed for cloud service mashups and integrates all these aspects into a practical formulation.

In [49], the CC trust to a CSP is related to the following parameters:

- Data location: CCs know where their data are actually located.
- Investigation: CCs can investigate the status and location of their data.
- Data segregation: Data of each CCs are separated from the others.
- Availability: CCs can access services and their data pervasively at any time.
- Privileged CC access: The privileged CCs, such as system administrators, are trustworthy.
- Backup and recovery: CSP has mechanisms and capacity to recover from catastrophic failures and not susceptible for disasters.
- Regulatory compliance: CSP complies with security regulations, certified for them and open for audits.

- Long-term viability: CSP has been performing the required standards for a long time.

The authors in [49] statistically analyze the results of a questionnaire answered by 72 CCs to investigate the perception of the CCs on the importance of the parameters above. According to this analysis, backup and recovery produces the strongest impact on a CC's trust in cloud computing followed by availability, privileged CC access, regulatory compliance, long-term viability and data location. Their survey showed that data segregation and investigation have weak impact on a CC's trust on cloud computing. In [33], the Authors propose giving controls to CCs, so they can monitor the parameters explained above [49]. They categorize these controls into five broad classes as controls on data stored, data during processing, software, regulatory compliance and billing. The techniques that need to be developed for these controls include remote monitoring, prevention of access to residual data, secure outsourcing, data scrambling, machine readable regulations and SLA, automatic reasoning about compliance, automatic collection of real time consumption data, and the capability of making your own bill. Although these are techniques which have already been developed for both cloud computing and the other purposes, many CSP still need time for their implementation, deployment and maturity. They also require quite an effort and expertise by CCs. Moreover, using these controls for all the services in a mashup may not always be practical. JRTM and TaaS Provider approach eliminates the requirement for the controls given to CCs for building trust.

In [5], risk is modelled in relation with trust. The *reliability trust* is defined as the probability of success and included into the risk based decision making process for a transaction. In [62], trust is introduced for assessing risks on the basis of organizational setting of a system. The trustworthiness of critical actors impacts on the probability of a risk scenario. [62] addresses this relation. JRTM links risk and trust, too. JRTM differs from these two models such that trust is calculated based on the probability that a CSP can eliminate a risk scenario. Moreover, JRTM is specifically designed for CSM while [5, 62] are for making investment decisions and managing critical systems like an air traffic control system.

Several frameworks have been proposed to assist users in service selection based on a variety of criteria such as QoS performance [56, 58], trust and reputation level [38, 43, 57, 59, 61] and privacy [16, 36]. Please note again that JRTM is not a service selection or service mashup configuration scheme. JRTM assess the risk level for a given CSM and makes recommendation if it is below the risk level acceptable by the

CC. JRTM can be used by a service selection scheme similar to the ones cited in this paragraph. The main difference of JRTM from the schemes listed above is that JRTM makes the recommendation based on risk and trust jointly by taking privacy, security and service risks together into account for a specific CSM.

Definitions

Before explaining JRTM in detail, we would like to introduce additional definitions for our model, and then to clarify the setting and the environment where JRTM can be used:

- Threat: A threat is the potential cause of an unwanted incident, which may result in harm to a system, person or organization.
- Vulnerability: Vulnerability is the weakness of an asset or control that can be exploited by a threat.
- Asset: An asset is something of value to the organization, which may be tangible (e.g., a building, computer hardware) or intangible (e.g., knowledge, experience, know-how, information, software, data).
- Control: A Control prevents or reduces the probability of a security, privacy or service incident (preventive or deterrent control), indicates that an incident has occurred (detective control) and/or minimizes the damage caused by an incident, i.e. reduces or limits the impact (corrective control).
- Personal data: Personal data relate to an individual who can be identified. The identification of the individual does not need to be directly. For example, there can be many people, whose name are John and were born on a certain date, but there may be only one John with that birth date and working in a certain company.
- Personally identifiable information (PII): PII are data that identify a person, such as social security number.
- Data subject: A data subject is an individual or organization who is the subject of personal data.
- Data controller: A data controller is an institution, organizational entity or person who alone or jointly with others determine the purposes and means of the processing of data.
- Incident: An incident is an event that results in a security, privacy or service violation/outage; e.g., respectively confidential data leakages after an attack, personal data collection without appropriate consent from the data subjects, or data cannot be recovered after a hardware failure.

- **Event:** An event is something that creates a vulnerability which may be exploited by a threat to compromise someone's asset(s). It is important not to confuse event with incident; For instance, losing an access badge is a security event. If an outsider uses the lost badge to enter a building without authorization, then it is an incident.
- **Security incident:** A security incident can be defined as a single attack or a group of attacks that can be distinguished from other attacks by the method of attack, identity of attackers, victims, sites, objectives or timing, etc. It results in the violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
- **Privacy Incident:** A privacy incident can be an intentional or unintentional violation of the consent obtained by the data controller from the data subjects, or a violation of the applicable data protection regulatory framework. A privacy incident can be the result of a security or service incident. For example, a data controller uses data for purposes not originally declared; an attacker gains access to personally identifiable information (PII); personal data is transferred to third parties without consent.
- **Service Incident -** A service incident is an event that violates the terms of service, service level agreement, or contracts between the CC and the CSP. It may be the result of failure (e.g. power outage, natural disaster, hardware failure, or human errors), attacks, or intervention of third parties (governmental agencies or law enforcement) preventing customers to use the services as established via contracts, resulting in service outages. Please note that we count the incidents caused by denial of service (DoS) attacks as security incidents, because their results are service outages.

A risk is a combination of the probability/likelihood of an incident and its impact/consequences. Since a risk is realized when threats exploit vulnerabilities, the probability of an incident is related to the existence of threats and vulnerabilities, as well as, the capabilities and willingness of the threats to exploit the vulnerabilities. On the other hand, the consequences depend on the assets owned by the subject, and it's security policy. In JRTM, the probability is based on the historic data related to the CSP performance, and the consequences are represented by means of the maximum incident probability acceptable by the CC, i.e., thresholds. If the impact on a data subject is high

(i.e., the value of the assets are high), lower thresholds are set.

JRTM is designed as a risk assessment tool for TaaS providers. A TaaS provider can be an organization like Cloud Security Alliance (CSA) or a certification agency in which all kinds of cloud ecosystem stakeholders are represented. Please note again that, JRTM alone is not for composing/configuring CSM or selecting a CSM. It assess if the risks related to a CSM are below the acceptable risk level for a CC. However, JRTM can also be used together with a service composition or selection tool. We explain how to do this in the next Section.

Joint trust and risk model for cloud service mashups

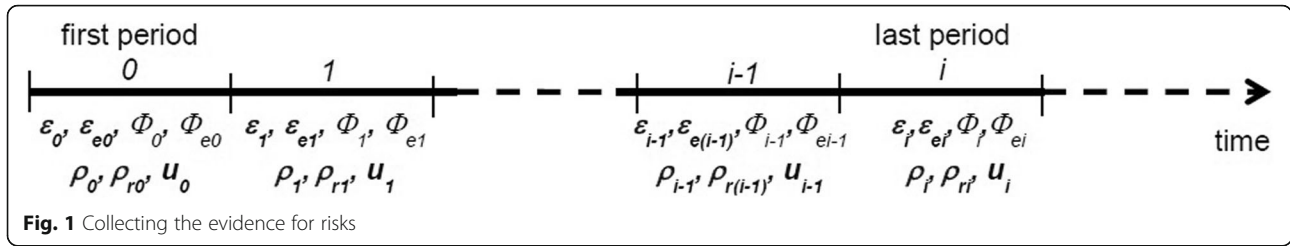
We first would like to highlight that JRTM is not an architecture or mechanism to build trust but a model that supports a CC to decide if a service mashup is trustworthy enough. In other words, our model computes if the risks associated with using a CSM is below the risk level that the CC is ready to accept. This model can be embedded into an overarching framework such as the one introduced in [54].

Collecting evidence for JRTM

JRTM is based on the CSP performance data collected by a TaaS provider. Evidence (i.e., performance data) are collected (i.e., counted) for periods as shown in Fig. 1. The length of the periods depends on the CSP dynamics, such as the number of subscribers and services, and may vary from the order of hours to the order of weeks.

For collecting evidences, the TaaS providers depend on the transparency by the CSP, i.e., the reports by the CSP. A CSP reports every event and incident to the TaaS provider as soon as they are detected. Note that JRTM is independent from the protocol and the means for reporting the events/incidents. This approach (i.e., CSP transparency to a TaaS provider) is more practical comparing to the approach that recommends giving controls to every CC [33], because:

- It is more secure for CSP comparing to the controls given to every CC. The probability that a TaaS provider makes use of controls to compromise the security or the performance of a cloud is lower.
- The TaaS provider does not need to share all the technical data with every CC. Therefore, CSP can protect both commercially and security wise sensitive data.
- CCs do not need to monitor or to control CSP for every cloud service. Instead, they take a



recommendation from a third party who is an expert on this topic.

- When TaaS providers are organizations accepted by the cloud industry, they may act also as a quality assurance mechanism. Therefore, accredited certification third parties can naturally become also a TaaS provider.

The TaaS provider approach assumes that accurate event and incident data can be collected by the TaaS providers. One may argue that this is not a realistic assumption because CSPs would not share this information with the TaaS providers. Therefore, our model also has a penalty scheme for the CSPs that do not report accurately. TaaS providers can detect false or incomplete incident reports during regular audits, triggering penalties. In addition to this, TaaS providers can use monitoring tools similar to the ones used for Monitoring as a Service, such as, Amazon Cloud Watch [1], Paraleap AzuroWatch [44], RackSpace CloudKick [48], Ganglia [37], Nagios [40], Zabbix [63], MonALISA [41] and GridICE [2]. Finally, there are already incident reporting frameworks such as ENISA Cloud Security Incident Reporting (CSIR) Framework [19]. A trust penalty scheme, such as the one in JRTM, can also complement frameworks like ENISA CSIR, and enforces accurate reporting of the incidents.

JRTM is a practical and scalable scheme that requires collection of only the following information (i.e., evidence) in every period:

- ϵ_i : the number of CCs who were subject to at least one security event in period i
- ϵ_{ei} : the number of CCs whose all security events were eliminated before they become incidents in period i
- ϕ_i : the number of CCs who were subject to at least one privacy event in period i
- ϕ_{ei} : the number of CCs whose all privacy events were eliminated before they become incidents in period i
- ρ_i : the number of CCs who were subject to at least one service event in period i

- ρ_{ei} : the number of CCs whose all service events are eliminated before they prevent achieving the SLOs defined in the SLA in period i
- u_i : the total number of CCs in period i
- D : the set of privacy event durations (i.e., the number of time periods between the time that a privacy event starts and the time that it is detected)

Two bytes suffice for storing each field of information listed above except for the last field, i.e., privacy event durations. Let's assume that the worst case for the privacy events occurs, which is 2^{16} privacy events in the last period. Then, we do not expect larger than 128 KB of data per CSP per period. If the periods are one day and there are 2^{10} CSPs registered in the TaaS Provider's database, the size of the data that the TaaS Provider needs to collect and store is around 128 MB, which is not much. Even if the number of CSPs in the database increases in the order of magnitude, the size of the data collected daily by the TaaS Provider stays around several GB.

As implied by the evidence collected, JRTM distinguishes three types of risks: security, privacy and service. Privacy has a difference from the other two. It is very likely that a privacy event is not detected when it is initiated. It is even probable that some of them may never be detected because their effect is not directly observable. On the other hand, the potential damage of a privacy event is higher when its duration is longer. Therefore, we collect evidence about privacy event durations and address this issue within our model. However, we cannot take undetected privacy events into account not only because they are not measurable but also because the TaaS providers' recommendations have to be based on evidence but speculations.

Computing risk and trust

The data collected by the TaaS need to be analyzed and assessed against various aspects of risk and trust. JRTM provides an aleatory approach for this purpose. Without a tool like JRTM, the collected data would not be very

easy to read, to understand and to compare, and therefore useful for many users. Moreover, such evaluation requires a qualitative or quantitative scale accepted and understood by the stakeholders.

In JRTM, risk and trust are modelled jointly by using the evidences. The real risk is the risk that cannot be (or is not) eliminated by the CSP. If the part of the security risk δ_e , privacy risk δ_ϕ and the service risk δ_ρ not eliminated by the CSP is lower than the CC can take (i.e., τ_e , τ_ϕ and τ_ρ), then the cloud service is viable for the CC. We further elaborate on this relation at the end of this section. As shown in (1), we perceive risk as the probabilities r_e , r_ϕ , and r_ρ that a security, privacy or service event occurs, and trust as the probabilities t_e , t_ϕ and t_ρ that the CSP can eliminate the events before they become security, privacy or service incidents.

$$\delta_x = r_x - (r_x \times t_x) \text{ for } x \in \{\varepsilon, \phi, \rho\} \tag{1}$$

This approach to model risk fits well for the dynamics in cloud computing because of two reasons: Firstly, it does not require that the TaaS provider assesses the consequence for the realization of a risk, which is very much dependent on the CCs' functions. Instead, the consequences are represented by the thresholds τ_e , τ_ϕ and τ_ρ given by the CCs. We discuss the selection of thresholds in Section "Due diligence and TaaS recommendation for accepting a service". Secondly, it does not need to assess all threats and vulnerabilities. For a TaaS provider or CC, it is not practical to list all threats and vulnerabilities because it is not likely that CSP will share all the details about their physical architecture, platforms and security systems with public, their CC or even with TaaS providers.

JRTM predicts the expected number of events by using the data about the past events as shown in Eqs. (2), (3) and (4). The periodical data related to risks r_e , r_ϕ , and r_ρ are weighted based on their freshness as given by (2), (3) and (4), where the Period i is the latest period, and $r_{e(i)}$, $r_{\phi(i)}$ and $r_{\rho(i)}$ are the current risk assessments for security, privacy and service respectively. The parameter ω in (2), (3) and (4) is the weight parameter, and can be given any value between 0 and 1 including 0 and 1 (i.e., $\{\omega \in \mathfrak{R} \mid 0 \leq \omega \leq 1\}$). The higher ω implies the lower level of uncertainty and the higher level of influence by the statistics in the last period. When it is 1, risk is determined based on the frequency of the incidents in the last period and there is not any uncertainty for the end result. When it is 0, risk is completely random according to the distribution and the statistics of the observations.

S in (2), P in (3) and G in (4) are random variables based on the probability distribution functions derived

from the statistical analysis of the observations on the ratios between security ε , privacy ϕ , service ρ events and the number of CCs u in that period respectively. The security, privacy and service event ratios (i.e., $s = \varepsilon/u$, $p = \phi/u$ and $g = \rho/u$) are fit to a distribution and statistics (i.e., shape, scale and location parameters), and this analysis for distribution and the statistics is repeated at the end of every period. The random variables $S: \Omega \rightarrow \mathfrak{R}^+$, $P: \Omega \rightarrow \mathfrak{R}^+$ and $G: \Omega \rightarrow \mathfrak{R}^+$ use these distributions and statistics in their probability spaces, i.e., $R_S(\Omega, \mathfrak{I}_S, P_S)$, $R_P(\Omega, \mathfrak{I}_P, P_P)$ and $R_G(\Omega, \mathfrak{I}_G, P_G)$, respectively. Ω is the set of positive real numbers including 0 (i.e., $\Omega \subset \mathfrak{R}$). \mathfrak{I}_S is the security event rate (i.e., the number of service events per user in a period), \mathfrak{I}_P is the privacy event rate, and \mathfrak{I}_G is the service event rate. P_S is the probability density function and statistics that fits best to the security event data set (i.e., $\{\varepsilon_0/u_0, \varepsilon_1/u_1, \dots, \varepsilon_i/u_i\}$), P_P is the probability density function and statistics that fits best to the privacy event data set (i.e., $\{\phi_0/u_0, \phi_1/u_1, \dots, \phi_i/u_i\}$) and P_G is the probability density function and statistics that fits best to the service event data set (i.e., $\{\rho_0/u_0, \rho_1/u_1, \dots, \rho_i/u_i\}$) collected for a CSP. Please note that the distribution and statistics for P_S , P_P and P_G include the data from the last period i .

$$r_{e(i)} = (1-\omega)S + \omega \frac{\varepsilon_i}{u_i}, \tag{2}$$

$$r_{\phi(i)} = (1-\omega)P + \omega \frac{\phi_i}{u_i}, \tag{3}$$

$$r_{g(i)} = (1-\omega)G + \omega \frac{\rho_i}{u_i}. \tag{4}$$

The uncertainties in Eqs. 2 to 4 are treated as aleatory by using random parameters. Stochastic uncertainties reflect variation in populations, and therefore imply the existence of knowledge (i.e., large and analyzed data set). That must be the reason why most of the available cloud risk assessments are based on epistemic uncertainty models, where uncertainties are due to the lack of knowledge. JRTM is developed for the mature stage of the cloud ecosystems, and therefore aleatory uncertainty approach is preferred.

For service risks, a stochastic model is a natural fit. However, security and privacy risks are in the essence not random but based on the deliberate acts by adversaries. Still, stochastic processes can be used and therefore very often used to model security and privacy risks when there is enough knowledge about their dynamics. However, randomization may not be appropriate to model security risks for special time periods, such as war, or for special type of security attacks designed by sophisticated attackers (i.e., first of its kind zero-day exploit attacks). We are working also on the application of the possibility and evidence theories instead of the

probability theory [30] for the special cases of security and privacy attacks.

We would like also to clarify one more time that we recommend categorizing events and incidents due to denial of service (DoS) attacks as in the service risk domain, because a DoS attack is designed to diminish the QoS or GoS, and therefore it is a service risk from the perspective of consequences.

As shown in Eq. 1, the risk is based on the number of expected events and the trust on CSP to eliminate them before they cause harm. We explained the stochastic process to calculate the number of expected events in the previous paragraphs. Now it is time to elaborate on the trust part of our equations. Nevertheless, before that we would like to introduce our penalty parameter α , which is for encouraging the CSPs to report the incidents timely and accurately. TaaS also collects the data about incidents from CCs and from the other sources such as ENISA CSIR framework [19]. TaaS Providers investigate the incidents reported by the other sources. If they find that a proven incident is not reported by a CSP, the trust value for the CSP decreases, which as a result increases the risk value for the CSP. In Eqs. (5) and (6), α_i is the penalty parameter for the CSP reporting accuracy in Period i , q_i is the number of incidents not reported by the CSP in Period i , and λ is the penalty degradation parameter which is a positive real number larger than or equal to one (i.e., $\{\lambda \in \mathbb{R} \mid \lambda \geq 1\}$) selected by CC similar to the slope value γ . TaaS providers assist CC to determine an appropriate slope value. The higher the penalty degradation parameter λ is, the quicker it takes to forget the inaccurate reporting by a CSP.

$$\alpha_c = \begin{cases} \lambda - 1 & , \text{if } \alpha_{i-1} = 0 \\ 1 & , \alpha_{i-1} \times \lambda > 1 \\ \alpha_{i-1} \times \lambda & , \text{otherwise} \end{cases} \quad (5)$$

$$\alpha_i = \begin{cases} \alpha_c & , \text{if } q_i = 0 \\ \frac{\alpha_{ci}}{q_i} & , \text{otherwise;} \end{cases} \quad (6)$$

Trust parameters t_e , t_ϕ and t_ρ consist of two parts, i.e., hard t_{eh} , $t_{\phi h}$, $t_{\rho h}$ and soft t_{es} , $t_{\phi s}$, $t_{\rho s}$, as shown in (7). Hard part of trust is based on the architecture (i.e., the security systems and capacity) of the CSP and the content of SLA. Therefore, it is mostly related to evidence, and we calculate it purely based on the performance of CSP. On the other hand, soft trust is sensitive to the latest incidents and more sensitive to negative incidents when compared to positive incidents. Typically trust and reputation are built slowly but can be lost very quickly. Please note that soft trust can be a negative value. Therefore, it is

added to the hard trust, and may have a negative or a positive effect in overall trust value. Apart from soft and hard part of the trust, we also have the penalty parameter α introduced in (5) and (6). We capture these relations through (7) to (15).

$$t_x = \begin{cases} 0, & \text{if } (t_{xh} + t_{xs}) \times \alpha < 0; \\ 1, & \text{if } (t_{xh} + t_{xs}) \times \alpha > 1; \\ (t_{xh} + t_{xs}) \times \alpha, & \text{otherwise.} \end{cases} \quad \text{for } x \in \{\varepsilon, \phi, \rho\} \quad (7)$$

Hard trust measurement is similar to risk assessment. In (8), (9) and (10), ε_{ei} , ϕ_{ei} and ρ_{ei} is the number of subscribers whose all security, privacy and service events are eliminated before they become incidents respectively at period i . Random variables $S_e: \Omega \rightarrow \mathbb{R}$, $P_e: \Omega \rightarrow \mathbb{R}^+$ and $G_e: \Omega \rightarrow \mathbb{R}^+$ generate random numbers according to the distributions and statistics of the ratios between the number of eliminated security events and total number of security events (i.e., $s_e = \varepsilon_e / \varepsilon$), the number of eliminated privacy events and total number of privacy events (i.e., $p_e = \phi_e / \phi$) and between the number of eliminated service events and the total number of service events (i.e., $g_e = \rho_e / \rho$). In (7), we have another random variable $R: \Omega \rightarrow \mathbb{R}^+$, which assigns random values according to the distributions and statistics of the values in privacy event duration set D . The probability spaces for S_e , P_e , G_e and R are similar to S , P and G except for the data used for the probability functions. Therefore, we are not giving their formal definitions here.

$$t_{eh(i)} = (1 - \omega)S_e + \omega \frac{\varepsilon_{ei}}{\varepsilon_i} \quad (8)$$

$$t_{\phi h(i)} = \left((1 - \omega)P_e + \omega \frac{\phi_{ei}}{\phi_i} \right)^R \quad (9)$$

$$t_{\rho h(i)} = (1 - \omega)G_e + \omega \frac{\rho_{ei}}{\rho_i} \quad (10)$$

Soft parts of trust $t_{es(i)}$, $t_{\phi s(i)}$ and $t_{\rho s(i)}$ are calculated based on the change in the performance of CSP. In Eq. (12), the slope value γ is a positive real number larger than or equal to one (i.e., $\{\gamma \in \mathbb{R} \mid \gamma \geq 1\}$) and represents the relation of trust with the negative/positive change (i.e., trend) in performance. If the performance of the CSP worsens, the CSP loses its credibility quickly. The sharpness of the drop in trust is related to the slope value γ . On the other hand, it takes more effort and time to gain trust as captured by (12).

$$d_{x(i)} = \frac{x_{ei} - x_{e(i-1)}}{x_i - x_{i-1}} \quad \text{for } x \in \{\varepsilon, \phi, \rho\}; \quad (11)$$

$$t_{xs(i)} = \begin{cases} d_{x(i)}^y, & \text{if } d_{x(i)} \geq 0; \\ -\sqrt[y]{|d_{x(i)}|}, & \text{if } d_{x(i)} < 0; \end{cases} \quad \text{for } \text{in}\{\varepsilon, \phi, \rho\} \tag{12}$$

Equation (1) captures risks for a single service. We extend them for CSMs in (13), (14) and (15), where A_S , A_P and A_G are the expected overall security, privacy and service risk (i.e., the risk that cannot be eliminated by the CSP) for CSMs respectively. The number of services in a CSM is n , and a_k is the number of alternative services available for service k in the inter-cloud (all the CSPs that can be accessed for this service). It is trivial to see at (13) and (14) that the higher the number of services compose a mashup, the higher the security and privacy risks become. The same relation can also be observed at (15) with a difference: the higher number of alternatives decreases the service risk. We examine these relations in more detail in Section “Experimental results”.

$$A_s = 1 - \prod_{k=1}^n (1 - \delta_{\varepsilon k}); \tag{13}$$

$$A_p = 1 - \prod_{k=1}^n (1 - \delta_{\phi k}); \tag{14}$$

$$A_G = 1 - \prod_{k=1}^n \left(1 - \prod_{m=1}^{a_k} \delta_{pkm} \right) \tag{15}$$

Since A_S , A_P and A_G are stochastic processes, their result are not deterministic (i.e., includes uncertainty through random variables). Therefore, a TaaS using our model first needs to build confidence intervals for A_S , A_P and A_G (i.e., $u(A_S) < A_S < v(A_S)$, $u(A_P) < A_P < v(A_P)$ and $u(A_G) < A_G < v(A_G)$) according to the confidence level λ given by the CC. For this, static Monte-Carlo simulation can be used. After building the confidence interval, the TaaS provider recommends the service mashup if and only if, $v(A_S) < \tau_\varepsilon$, $v(A_P) < \tau_\phi$ and $v(A_G) < \tau_\rho$, where τ_ε , τ_ϕ and τ_ρ are the security, privacy and service risk thresholds agreed with the CC.

We would like to highlight that JRTM analyzes δ_ε , δ_ϕ , δ_ρ for a CSP but not for a service. However, when A_S , A_P or A_G are being assessed, the services in the mashup may be coming from different CSP, and JRTM can compute the risk accordingly. Please note that composing a service mashup is not the aim of JRTM. JRTM is not a scheme to compare alternative service mashups, either. The purpose of JRTM is to assess if the risk of a CSM is below the acceptable level for a CC. However, the services of a TaaS provider that employs JRTM can be used by another service for mashup composition [10] and selection, because JRTM does not only assess if the risk of a

service is acceptable but also assigns probabilities for security, privacy and service risks. Therefore, JRTM can be integrated into a “multi-criteria decision making with posterior articulation of user preferences [11]” algorithm as follows:

Step 1: The set $S = \{CSM_1, CSM_2, \dots, CSM_n\}$ of alternative CSM for a CC is given.

Step 2: JRTM computes security, privacy and service risks for each CSM in S .

Step 3: The CSMs assessed as too risky (i.e., at least one of the security, privacy or service risk probabilities for the CSM is higher than the thresholds) are removed from S , which creates the set S' of feasible CSM, i.e., $S' \subset S$.

Step 4: If $S' = \emptyset$ (i.e., S' is an empty set), the CC is informed that there is no feasible CSM in S and the process ends.

Else if $|S'|=1$ (i.e., S' has only one element), the CC is informed about the only feasible CSM and the process ends.

Step 5: If CC is interested in only one risk domain (i.e., security, privacy and service), the CSMs in S' is ordered according to that domain, and the CC is informed about the best CSM, which may be more than one if multiple CSM has the same score. Please note that this is very unlikely.

Else the non dominated set S'' of feasible CSMs, $S'' \subset S'$, is created. In S'' , there is no CSM, which is worse in all risk domains comparing to another CSM in S'' , i.e., there is no CSM dominated by another CSM. After this the CC is informed with S'' for posterior articulation of CC preferences.

Step 6: The process ends.

Due diligence and TaaS recommendation for accepting a service

To be complete, two further questions need to be answered: How can a CC determines τ_ε , τ_ϕ and τ_ρ ? How can a TaaS provider assign the distributions and statistics for S , P , G , S_ρ , P_ρ , G_ρ and R when a CSP is registered first time?

JRTM is in essence based on the expected rate of security, privacy and service incidents with some adjustments related to the tendency (i.e., increasing or decreasing incident rates). Therefore, risk thresholds for JRTM are intuitively clear and an experienced TaaS provider can make suggestions for them based on the assets [18] that the CC would like to process or to store in the cloud. Then the CC either agrees with or can ask justifications on them. When the thresholds are agreed, the TaaS provider’s recommendation is that the assessed absolute risk is below the risk acceptable by the CC. Hence, the acceptable level of risk is understood and

agreed by the correct party, i.e., the CC, and can also be based on a relative risk analysis [32]. For this, CCs do not need to know the details about the technical architectures, their vulnerabilities and threats. Instead they focus on a comprehensive and abstract risk probability given based on practical evidence. Therefore, it is easier for a CC to run a risk assessment based on the consequences and opportunities of the risks taken. A number of recommendations may guide TaaS providers and CCs in the definition of the risk profiles [18, 52].

There are multiple ways to answer the second question. The TaaS provider can initialize S, P, G, S_e, P_e, G_e and R with the same distributions and statistics as the average of the other CSP that have a similar architecture to the CSP registered the first time. After this, the CCs may be provided with a recommendation by using larger confidence intervals than the confidence level specified by the CCs and warned about this fact.

Another difficulty in making the statistics is related to temporal and geographic correlations of the risks. For example, a law such as “the data protection act” affects not only one CSP but all CSP that have data center in the same

country. Therefore, the impacts of this law should not be reflected only to a CSP that has the experience due to this law but also all the CSPs that have a data center in the same country. Similarly, when this law changes or is removed, its effects should be removed from the statistics associated with all the CSP in the country. None of these changes the essence of JRTM.

Experimental results

We run experiments by using Monte-Carlo simulation methodology for three purposes: to have better insight into our models; to examine the relations between independent engineering variables (i.e., freshness (ω), slope (γ) and period length) and dependent variables (i.e., confidence intervals for security S , privacy P and service S risks); and, more importantly, to verify our models. A subset of results from our experiments are depicted and analyzed in this section. For the experiments, we generated random values for S, P, G, S_e, P_e, G_e and R . We factored our experiments for the Poisson and Normal distributions and expected values to analyze the sensitivity of the model

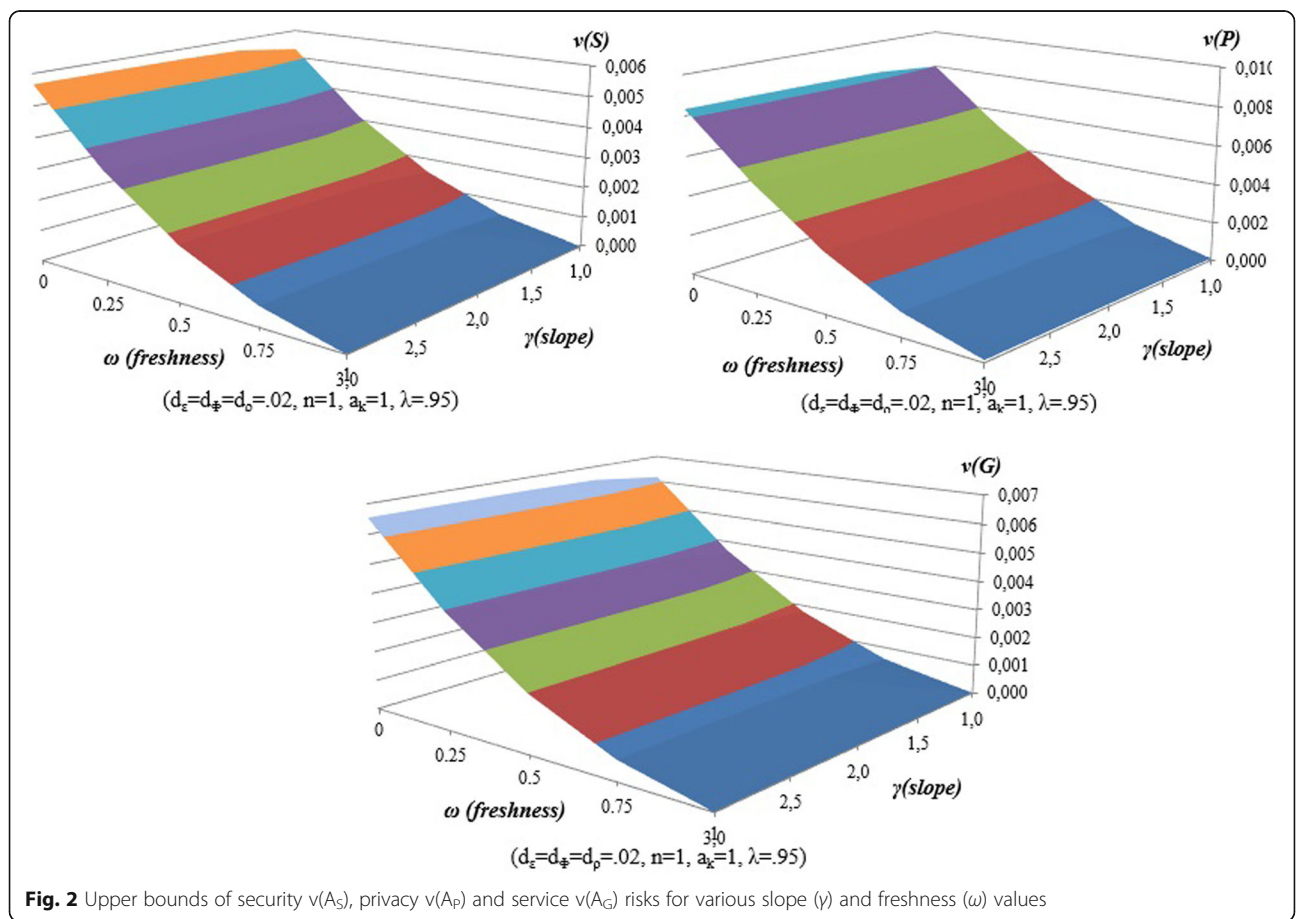


Fig. 2 Upper bounds of security $v(A_S)$, privacy $v(A_P)$ and service $v(A_G)$ risks for various slope (γ) and freshness (ω) values

against the statistical characteristics of our random variables. Because of the stochastic nature of our model, we repeated each experiment 50 times and constructed the confidence intervals. For the other independent variables, we changed their value according to our design of experiment, which is based on partial factoring. The details about the value ranges for our factoring parameters are clarified below, where we analyze and explain some of the results.

In Fig. 2, the sensitivity of security A_S , privacy A_P and service A_G risks against the changes in independent engineering variables freshness (ω) and slope (γ) are depicted. S , P and G are distributed according to Poisson distribution with 0.02, which means 2% percent of users were subject to a security, privacy or a service event in every period. In the last period, the CSPs managed to eliminate 95% of all these events before they become an incident. In the previous period, this value is 93%. This indicates 2% improvement in the performance of CSPs in the average (i.e., the success in eliminating events before they become incidents), which affects the soft trust according to the slope (γ) value.

As shown in Fig. 2, the effect of the changes in slope value is not much, because it changes only the soft trust, which should not contribute to the risk perception in a major way when the change in CSP performance is only 2% and positive. Most probably this would be unrecognizable. On the other hand, the effect of the freshness (ω) parameter is significant. The reason for that is the change in the number of events. In our experiments, the number of events in the last period goes down from 0.02 to 0.002. With the effect of soft trust, the model calculates risks as almost 0, except for privacy, when risk perception is based on only the events that happened in the last period.

In the privacy risk calculation, the duration of incidents before they get detected is also an important parameter. In the experiments for the results shown in Fig. 2, the duration is Poisson distributed with 3 period lengths in the average. Therefore, the privacy risk P is always above 0.0001 and around 60% higher comparing to the security and service risks.

The difference of the experiments in Fig. 3 with respect to Fig. 2 is the change in the performance of CSPs.

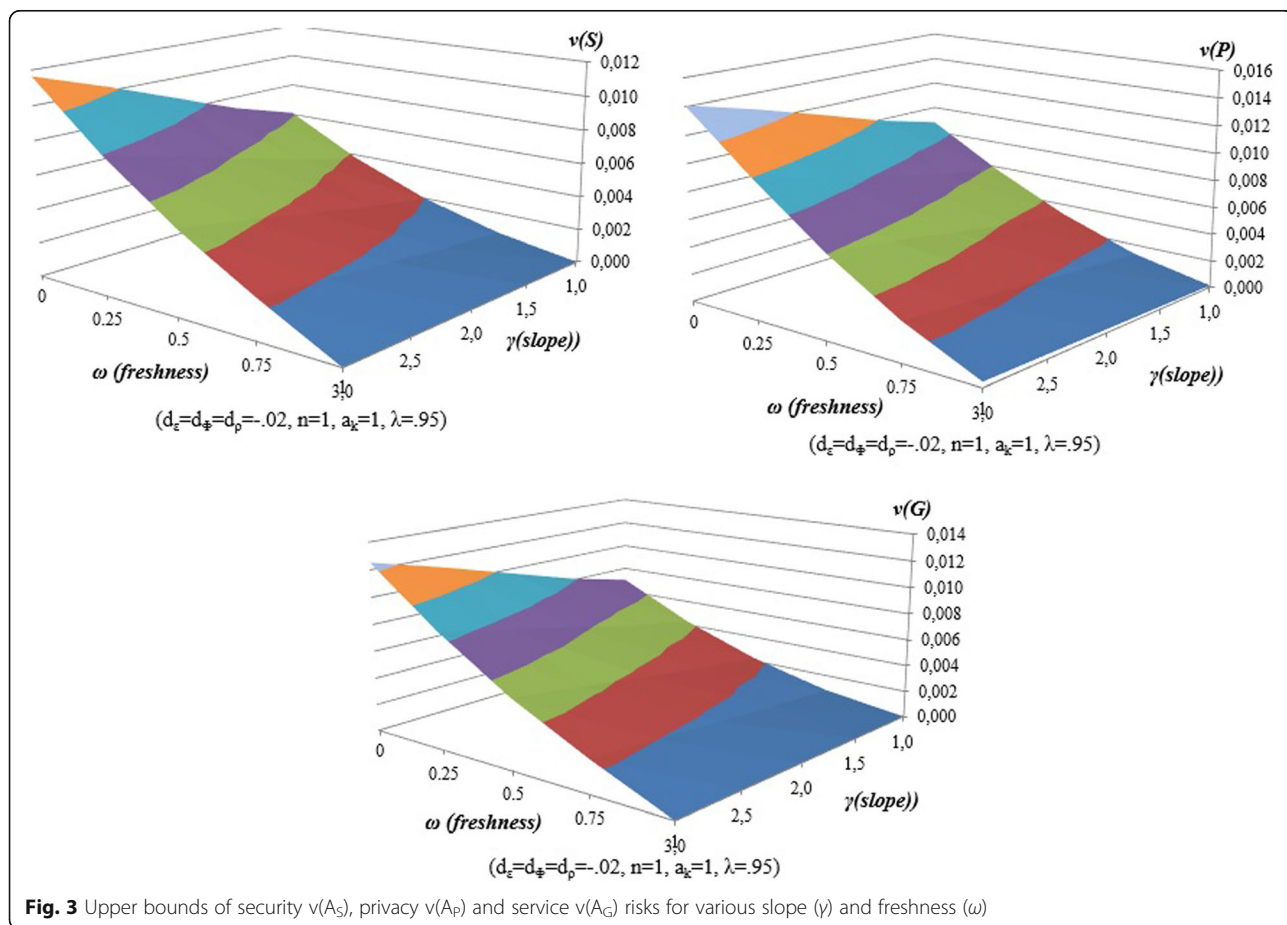


Fig. 3 Upper bounds of security $v(A_S)$, privacy $v(A_P)$ and service $v(A_G)$ risks for various slope (γ) and freshness (ω)

In Fig. 2, it is 0.2 and positive. In Fig. 3, it is again 0.2, but this time it is negative, which means that the CSPs become less successful in eliminating the events before they become incidents (i.e., it goes down from 95% to 93%). The impact of this is trivial and the model captures it very well. First, the soft trust reduces because this is a negative performance change, and therefore the slope γ becomes more effective at the risk perception. This is more significant when freshness ω is higher. Nevertheless, the relation between freshness and slope are not direct but indirect. When the risk perception is higher, the effect of soft trust and therefore the slope also becomes higher. Except for these differences, the other relations between the independent and dependent variables in Fig. 3 are almost the same as in Fig. 2.

If the slope value is higher, the improvement in CSP performance is reflected to the risk perception slowly, on the other hand, the degradation in CSP performance is reflected to the risk perception more aggressively. Therefore, there is always a positive relation with risk and slope γ , which means that the higher the slope value becomes, the higher the risk is perceived independent from the tendency in the CSP performance. This

behaviour is exactly what we expect from our model, and observable in Figs. 2, 3 and 4.

In Fig. 4, we examine the relation between slope and the tendency in CSP performance more closely. We assign 0.85 for the event elimination performance in the period before the last period. Then, we change the event elimination rates between 0.95 and 0.75 for the last period.

When there is no change in the CSP performance, changing the slope value does not affect the risk perception. That is not a surprise, because slope is for amplifying the effects of the performance change on the soft trust. When the tendency is positive, which means the performance of the CSP gets better in eliminating events, the effect of the slope at the risk perception is less comparing to the negative tendency. Trust can be gained slowly and lost more quickly. Therefore, we can tell that our model addresses the soft trust effect as expected and explained in Section “Related work and definitions”.

In Fig. 5, the relation between the number of services and risk is depicted for the same values as the ones used for the experiments in Figs. 2 and 3. As

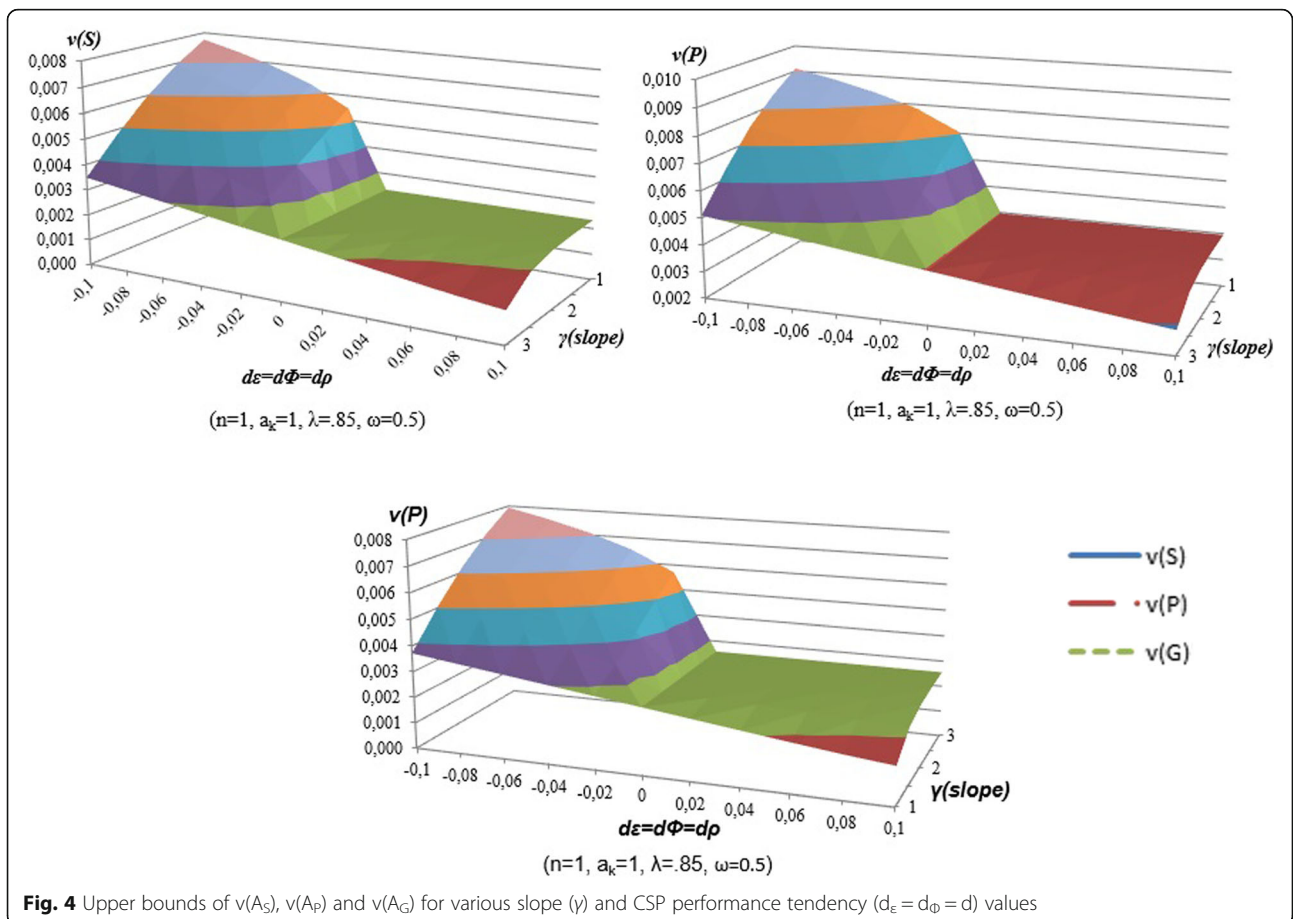


Fig. 4 Upper bounds of $v(A_S)$, $v(A_P)$ and $v(A_G)$ for various slope (γ) and CSP performance tendency ($d_\epsilon = d_\phi = d_p$) values

illustrated in Fig. 5, there is a linear relation, and the privacy risk is the most sensitive against the number of services.

We also examine the sensitivity of risk against the number of alternative services (i.e., available services for the same service type within the inter-cloud.) We observe that the number of alternative services does not change the security or privacy risks. However, it impacts on the service risk. When there is one alternative service in the average for each type of service in a mashup made up of 11 service types, the service risk is calculated as 0.0191. When the average number of alternatives becomes two, the service risk goes down to 0.0001. When it is three in the average, the risk becomes almost zero.

Figure 6 shows the sensitivity of the privacy risk against the average duration of events before they are detected. Please note that the security and service risks are not sensitive against the event duration. In our tests, we examine the sensitivity of JRTM not only against the average duration length but also the change in duration length distribution (i.e., Poisson distribution and Normal distribution with various standard deviations). We observed an interesting result for Normal distribution. When standard deviation is as large as the average, the risk perception gets higher. This fits with the intuition because the higher variation means the higher uncertainty. Nevertheless, when the average gets higher, the higher standard deviation may reduce the risk because it also implies the lower privacy event durations.

Figure 7 depicts the security $v(A_S)$, privacy $v(A_P)$ and service $v(A_G)$ risks for various period lengths. Figure 7 also shows the sensitivity of the model against the changes in the event rates, because the longer the period length becomes, the higher the number of events are observed in each period.

In Fig. 7, we also analyse the effect of changing the distribution for the event occurrence. When we apply

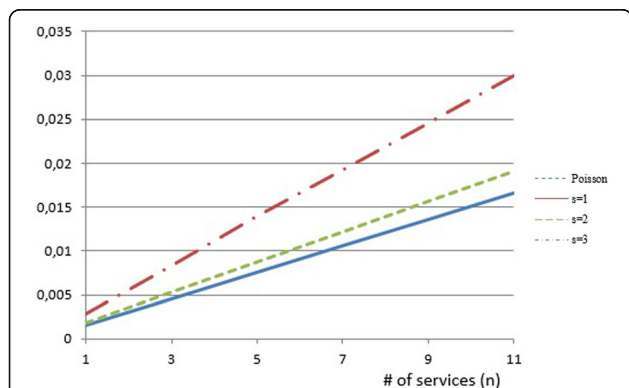


Fig. 5 Upper bounds of security $v(A_S)$, privacy $v(A_P)$ and service $v(A_G)$ risks for various number of services n in cloud service mashup

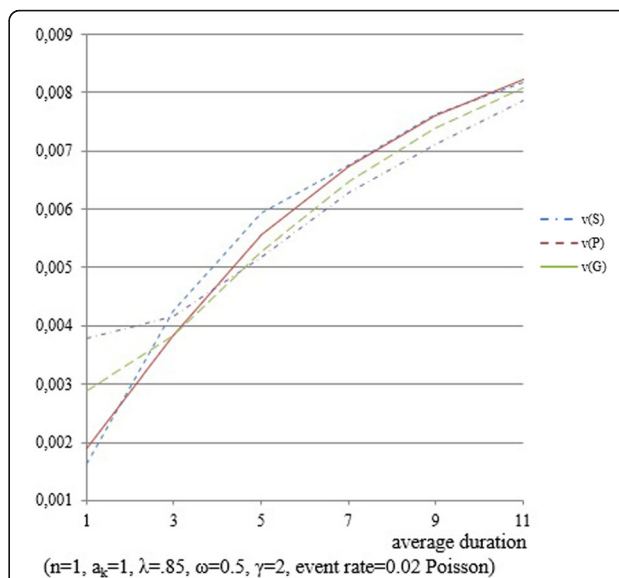
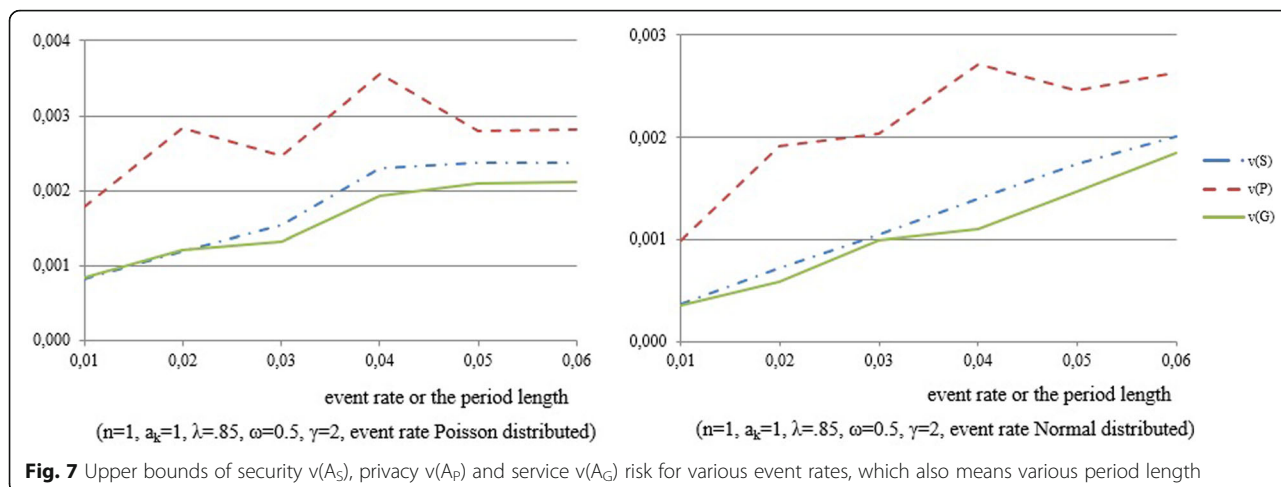


Fig. 6 Upper bounds of privacy risk $v(A_P)$ for various average durations of privacy incidents

the same average rates, the risks calculated for the Normal distribution is higher. Please note that we assign a standard deviation equal to 10% of the average for the Normal distribution. We observe an anomaly at the plots for privacy risk $v(A_P)$ in Fig. 7. The privacy risk reduces at several points when the event rate gets higher. That is because we do not increase the event rate but the period length which causes the event durations in the number of periods are reduced when period lengths are increased. When privacy event duration is reduced, that decreases privacy risk. Therefore, we observe a decrease in privacy risk although the event rate increases.

In Fig. 8, the sensitivity of the model against the changes in the penalty parameter α is depicted. Please remember that the penalty parameter is for encouraging the CSPs to report incidents more timely and accurately. As expected there is a linear relation between the risk values and the penalty parameter, and the effect of a decrease in penalty value significantly decreases the trust and increases the risk. This is exactly what the parameter is designed for, and therefore verifies the model. There is an interesting observation from Fig. 8: The privacy risk is the highest comparing to the service and security risks when no penalty is applied (i.e., the penalty value is 1). The higher the penalty is (i.e., the penalty value decreases), the lower the difference between the service and privacy risks becomes. For penalty values 0.1, 0.2 and 0.3, the service risk is higher than the privacy risk. The reason for this is the effect of the trust in the model.



Privacy risk does not decrease as much as the other risks when the trust value becomes higher, because the probability that a privacy incident cannot be detected is higher comparing to the service and security risks. Therefore, when the penalty reduces the positive effect of the trust in the model, security and service risks become higher than privacy risk.

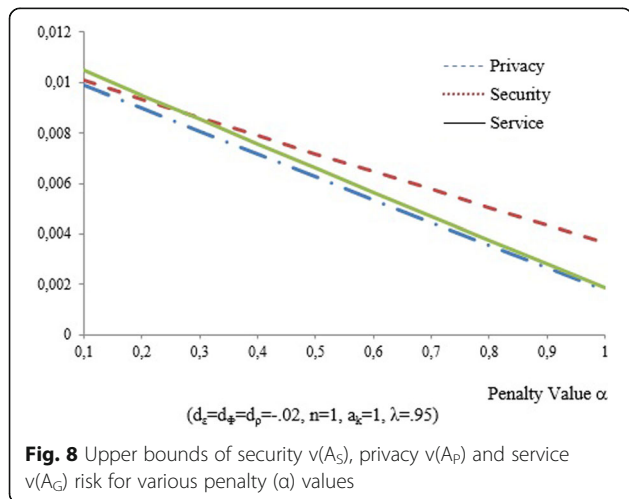
In Fig. 9, the likelihood for privacy, security and service risks are given for 44 CSPs registered in Security Trust and Assurance Registry (STAR) [15] by Cloud Security Alliance (CSA). Almost 300 CSP provided information about how they implemented controls for the security, privacy and service assurance in the STAR. The likelihood value is the result of Cloud Adopted Risk Assessment Model (CARAM) [11], which aggregates the ENISA likelihood assessment [18] for cloud risks into

three domains (i.e., security, privacy and service) and applies to CSPs based on the data in STAR. The scale used for likelihood is between 0 and 9. CARAM results are not based on the historic data but vulnerabilities and threats assessed by ENISA and the controls implemented by the CSPs. However, we can observe that privacy risk is higher than security and service risks, which are close to each other, almost for every CSP. This supports the JRTM results depicted in Figs. 7 and 8.

Conclusions

Risk and trust are critical notions for cloud services and closely related to each other. In literature, trust is stated as the main barrier for potential subscribers before they embrace cloud services. For realization of cloud computing, trust relation between the CC and the CSP has to be established. This requires an in depth understanding of risk and the accountability of the CSP. Cloud service mash-ups exacerbate the complexity of accountability, risk and trust relations among the CC and the CSP. Therefore, practical services possibly in the form of TaaS are required. A TaaS provider may use the data about the reputation of a CSP, and the risk constraints of the subscribers, to recommend or not to recommend a specific service to a subscriber.

A joint trust and risk model based on statistical data is introduced for this purpose. The model, i.e., JRTM, addresses not only the security related risks but also the risks related to privacy and the performance of the services. It is amenable to the automated treatment, allowing to represent the service chain, and to dynamically monitor risk thresholds, according to profiles established with the CC. JRTM differentiates the negative performance from the positive performance in risk assessment based on the CC preferences. It also takes into account



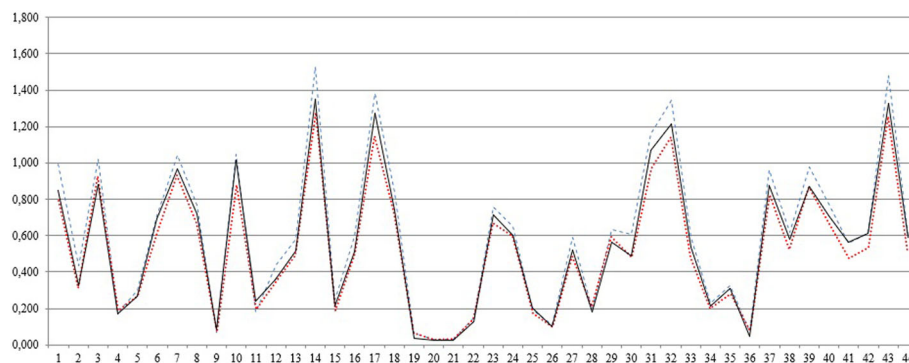


Fig. 9 The probability values calculated by CARAM for 44 CSPs in STAR

the freshness of the data about the performance of the CSP again according to the parameters specified by the CC. The model is practical for a TaaS and for cloud service mashups. Our initial experimentation verifies that our model is aligned with the perception of risks and trust as explained in the literature.

Abbreviations

CAIQ: Cloud Assessment Initiative Questionnaire; CARAM: Cloud Adoption Risk Assessment Model; CC: Cloud Customer; CCM: Cloud Control Matrix; CNIL: The Commission nationale de l'informatique et des libertés; CSA: Cloud Security Alliance; CSIR: Cloud Security Incident Reporting; CSM: Cloud Service Mashup; CSP: Cloud Service Provider; DoS: Denial of Service; ENISA: European Network and Information Security Agency; GoS: Grade of Service; IEC: International Electrotechnical Commission; ISACA: Information Systems Audit and Control Association; ISO: International Organization for Standardization; IT: Information Technology; JRTM: Joint Risk and Trust Model; PII: Personally Identifiable Information; QoS: Quality of Service; SLA: Service Level Agreement; SLO: Service Level Objectives; STAR: Security, Trust and Assurance Registry; TaaS: Trust as a Service

Acknowledgements

This work is conducted as part of the EU-funded FP7 project titled as "Accountability for Cloud and Other Future Internet Services" (A4Cloud) under grant agreement number 31755 which introduces an accountability-based approach for risk and trust management in cloud ecosystems.

Funding

University of Stavanger funds the publication of this paper.

Availability of data and materials

There is no data available specifically for this paper. Our research benefited from the other datasets such as CSA STAR.

Authors' contributions

The paper is the common effort of the both authors in all sections. Both authors read and approved the final manuscript.

Authors' information

Erdal Cayirci, PhD, is a professor at University of Stavanger in Norway and the CEO of DataUniTor AS. His research interests include modelling and simulation, data analytics, security, privacy, cloud computing, blockchain and mobile communications.

Anderson Santana de Oliveira, PhD, is a Researcher in the Product Security Research team, working on Data Protection, Privacy and security topics. His research interests include cloud computing, data protection, privacy, accountability, trust and risk assessment.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Author details

¹Electrical Engineering and Computer Science Department, University of Stavanger, Stavanger, Norway. ²SAP Security Research, Mougins, France.

Received: 30 November 2017 Accepted: 29 June 2018

Published online: 02 August 2018

References

1. Amazon CloudWatch, <http://aws.amazon.com/cloudwatch/>
2. Andreozzi S, De Bortoli N, Fantinel S, Ghiselli A, Rubini GL, Tortone G, Vistoli MC (2005) Gridice: a monitoring service for grid systems. *Future Gener Comput Syst* 21(4):559–571
3. Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M (2010) A view of cloud computing. *Commun ACM* 53(4):50–58
4. Asnar A, Zannone N (2008) Perceived risk assessment. In *Proceedings of the 4th ACM Workshop on Quality of Protection (QoP)*, p 59–64
5. Audun J, Presti SL (2004) Analysing the relationship between risk and trust. In *Proceedings of the 2nd International Conference on Trust Management (iTrust)*, p 135–45
6. Banerjee S, Mattmann C, Medvidovic N, Golubchik L (2005) Leveraging architectural models to inject trust into software systems. In: *Proc. SESS '05*. ACM, New York, pp 1–7
7. Buyya R, Ranjan R, Calheiros RN (2010) InterCloud: Utility-oriented Federation of Cloud Computing Environments for Scaling of Application Services. *Proceedings of the 10th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP'10)*, pp 13–31
8. Cayirci E (2013) A Joint Trust and Risk Model for MSaaS Mashups. In: Pasupathy R, Kim S-H, Tolk A, Hill R, Kuhl ME (eds) *Proceedings of the 2013 Winter Simulation Conference*. Institute of Electrical and Electronics Engineers, Inc, Piscataway, New Jersey.
9. Cayirci E (2013) Modelling and Simulation as a Service: A Survey. In: Pasupathy R, Kim S-H, Tolk A, Hill R, Kuhl ME (eds) *Proceedings of the 2013 Winter Simulation Conference*. Institute of Electrical and Electronics Engineers, Inc, Piscataway, New Jersey.
10. Cayirci E (2013) "Configuration Schemes for Modelling and Simulation as a Service Federations," *Simulation Transactions of the Society for Modelling and Simulation International*. 89(11):1388–1399
11. Cayirci E, Garaga A, de Oliveira AS, Roudier Y (2016) A risk assessment model for selecting cloud service providers. *J Cloud Computing* 5:14
12. CNIL, "Methodology for Privacy Risk Management: How to Implement the Data Protection Act," 2012, <https://www.cnil.fr/en/media>, June 2014
13. CSA, "Consensus Assessment Initiative Questionnaire (CAIQ)," <https://cloudsecurityalliance.org/research/caiq/>. Accessed 23 July 2018.
14. CSA, "The Notorious Nine Cloud Computing Top Threats in 2013," https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf. Accessed 23 July 2018.

15. CSAN, "Security, Trust & Assurance Registry (STAR)," https://cloudsecurityalliance.org/star/#_registry. Accessed 23 July 2018.
16. Costante E, Paci F, Zannone N (2013) Privacy-aware web service composition and ranking. In Proceedings of the 20th IEEE Conference on Web Services (ICWS), p 131–38
17. DHS. (2008) DHS risk lexicon. Department of Homeland Security
18. ENISA. (2009). Cloud computing: benefits, risks and recommendation for information security
19. ENISA. (2013). Cloud security incident reporting: framework for reporting about major cloud security incidents
20. Ezell BC, Bennet SP, Von Winterfeldt D, Sokolowski J, Collins AJ (2010) Probabilistic risk analysis and terrorism risk. *Risk Anal* 30(4):575–589
21. Gadia S (2011) Cloud computing risk Assessment: a case study. *ISACA Journal* 4:1–6
22. Garg, S.K., S. Versteeg, and R. Buyya. 2011. "SMICloud: a framework for comparing and ranking cloud services." Fourth International Conference on Utility and Cloud Computing
23. Gupta R, Prasad K, Luan L, Rosu D, Ward C (2009) Multi-dimensional knowledge integration for efficient incident Management in a Services Cloud. In Proceedings of the IEEE International Conference on Services Computing (SCC), p 57–64
24. Hwang K, Fox G, Dongarra J (2011) Distributed and cloud computing. Morgan Kaufmann Publishers, San Francisco
25. IEC 62198, "Managing Risk in Projects – Application Guidelines," <http://webstore.iec.ch/webstore/webstore.nsf/artnum/048815lopdocument>. Accessed 23 July 2018.
26. ISACA, "COBIT 5: A Business Framework for the Governance and Management of Enterprise IT," <http://www.isaca.org/cobit/pages/default.aspx>. Accessed 23 July 2018.
27. ISO 31000, "Risk Management (2009)," <http://www.iso.org/iso/home/standards/iso31000.htm>. Accessed 23 July 2018.
28. ISO/IEC 31010, "Risk Management-Risk Assessment Techniques (2009)," <https://www.iso.org/obp/ui/#iso:std:iec:31010:ed-1:v1:en>. Accessed 23 July 2018.
29. Jansen W, Grance T (2011) Guidelines on security & privacy, draft special publication 800–144 NIST. Department of Commerce, US
30. Jøsang A (2001) A logic for uncertain probabilities. *International journal of uncertainty, Fuzziness and Knowledge-Based Systems* 9(3):279–311
31. Kandukuri, B.R., R. Paturi, and V.A. Rakshit. 2009. "Cloud security issues." IEEE International Conference on Services Computing
32. Kaplan S, Garrick BJ (1981) On the quantitative definition of risk. *Risk Anal* 1(1):11–27
33. Khan, K. and Malluhi, Q. 2013. "Trust in Cloud Services: Providing More Controls to Clients," IEEE Computer, July
34. Li W, Ping L (2009) Trust model to enhance security and interoperability of cloud environment. In Proceedings of the 1st IEEE Cloud Computing Conference (CloudCom), p 69–79
35. Marsh S (1994) Formalising trust as a computational concept. Doctoral dissertation, University of Stirling, Scotland UK
36. Massacci F, Mylopoulos J, Zannone N (2006) Hierarchical hippocratic databases with minimal disclosure for virtual organizations. *VLDB J* 15(4):370–387
37. Massie ML, Chun BN, Culler DE (2004) The ganglia distributed monitoring system: design, implementation and experience. Vol 30. Elsevier Parallel Computing, pp 817–40
38. Maximilien M, Singh MP (2004) Toward autonomic web services trust and selection. In: Proceedings of the 2nd international conference on service oriented computing (ICSOC '04). ACM, New York, pp 212–221
39. Mayer RC, Davis JH, Schoorman FD (1995) An integrative model of organizational trust. *Acad Manag Rev* 20(3):709–734
40. Nagios, <http://www.nagios.org/>. Accessed 23 July 2018.
41. Newman HB, Legrand IC, Galvez P, Voicu R, Cirstoiu C (2003) Monalisa : a distributed monitoring service architecture. In: Proceedings of CHEPO3, LaJolla, USA
42. Osterwalder D (2001) Trust through evaluation and certification. *Soc Sci Comput Rev* 19(1):32–46
43. Paradesi S, Doshi P, Swaika S (2009) Integrating behavioral Trust in web Service Compositions. In Proceedings of the IEEE International Conference on Web Services, p 453–60
44. Paraleap AzureWatch, <https://www.paraleap.com/AzureWatch>. Accessed 23 July 2018.
45. Pearson S (2012) Privacy, security and Trust in Cloud Computing. In: Pearson S, Yee G (eds) Privacy and security for cloud Computing, computer communications and networks. Springer-Verlag, New York, pp 3–42
46. Pearson S, Charlesworth A (2009) Accountability as a way forward for privacy protection in the cloud. In: Jaatun MG, Zhao G, Rong C (eds) Proceedings of the 2009 CloudCom. Springer-Verlag, New York, pp 131–144
47. Pearson S, Tountopoulos V, Catteddu D, Südholt M, Molva R, Reich C, Fischer-Hübner S, Millard C, Lotz V, Jaatun MG, Leenes R, Rong C, Lopez J (2012) Accountability for cloud and other future internet services. In Proceedings of the 4th IEEE Cloud Computing Conference (CloudCom), p 629–32
48. RackSpace Cloud Monitor, <http://www.rackspace.com/cloud/monitoring/>
49. Rashidi A, Movahhedinia N (2012) A model for user trust in cloud computing. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)* 2(2):1–8
50. Rousseau D, Sitkin S, Burt R, Camerer C (1998) Not so different after all: a cross-discipline view of trust. *Acad Manag Rev* 23(3):393–404
51. Ryan KLK, Jagadpramana P, Mowbray M, Pearson S, Kircheng M, Liang Q, Lee BS (2011) TrustCloud: a framework for accountability and Trust in Cloud Computing. In: 2nd IEEE cloud forum for practitioners (ICFP)
52. Simmonds, P., Chris Rezek, & Archie Reed. (2011). Security Guidance for Critical Areas of Focus in Cloud Computing V3.0 (No. 3.0) (p. 177). Cloud Security Alliance. Retrieved from <http://www.cloudsecurityalliance.org/guidance/>
53. Singh S, Morley C (2009) Young Australians' privacy, security and Trust in Internet Banking. In: Proceedings of the 21st Annual Conference of the Australian Computer-Human interaction Special interest Group: Design: Open 24/7
54. Singhal M, Chandrasekhar S, Tingjian G, Sandhu RS, Krishnan R, Ahn G-J, Bertino E (2013) Collaboration in multicloud computing environments: framework and security issues. *IEEE Computer Magazine* 46(2):76–84
55. Toosi AN, Calheiros RN, Thulasiram RK, Buyya R (2011) Resource provisioning policies to increase IaaS Provider's profit in a federated cloud environment. In the Proceedings of the IEEE International Conference on High Performance Computing and Communications (HPCC), p 279–87
56. Tran WX, Tsuji H (2008) QoS based ranking for web services: fuzzy approaches. In: Proceedings of the 2008 4th international conference on next generation web services practices (NWESP '08). IEEE computer society, Washington, DC, USA, pp 77–82
57. Vu L-H, Hauswirth M, Aberer K (2005) QoS-based service selection and ranking with trust and reputation management. In: Proceedings of the 2005 confederated international conference on on the move to meaningful internet systems (OTM'05). Springer-Verlag, Berlin, Heidelberg, pp 466–483
58. Wang P, Chao K-M, Lo C-C, Huang C-L, Li Y (2006) A fuzzy model for selection of QoS-aware web services. In: Proceedings of the IEEE international conference on e-business engineering (ICEBE '06). IEEE computer society, Washington, DC, USA, pp 585–593
59. Wang P, Chao K-M, Lo C-C, Farmer R, Kuo P-T (2009) A reputation-based service selection scheme, e-Business Engineering. In: IEEE International Conference on ICEBE '09, pp 501–506
60. Wang Y, Lin K-J (2008) Reputation-oriented trustworthy computing in E-commerce environments. *Internet Computing* 12(4):55–55
61. Xu Z, Martin P, Powley W, Zulkernine F (2007) Reputation-enhanced QoS-based web services discovery. In: IEEE International Conference on web services. ICWS 2007, pp 249–256
62. Asnar Y, Giorgini P, Massacci F, Zannone N (2007) From trust to dependability through risk analysis. In Proceedings of the 2nd International Conference on Availability, Reliability and Security (ARES), p 19–26
63. Zabbix, <http://www.zabbix.com/>. Accessed 23 July 2018.