Proceedings of the 2013 Winter Simulation Conference
R. Pasupathy, S.-H. Kim, A. Tolk, R. Hill, and M. E. Kuhl, eds

A JOINT TRUST AND RISK MODEL FOR MSAAS MASHUPS

Erdal Cayirci

Electrical Engineering & Computer Science Department
University of Stavanger
Stavanger, 4036, NORWAY

ABSTRACT

Modeling and simulation as a service and its difference from software as a service is explained. The literature on trust and risk for cloud service mash-ups are surveyed. A joint trust and risk model is introduced for MSaaS federations. The model is based on historic data related not only security incidents but also performance records. Negative and positive performances are differentiated and the freshness of the historic data are taken into account in the model. A numerical analysis by using the model through Monte-Carlo simulation is also provided.

1 INTRODUCTION

Modelling and simulation as a service (MSaaS) has attracted many researchers recently. Virtualization and cloud computing have already been used as infrastructure and platform both for military and civilian modelling and simulation (M&S) (Cayirci and Rong 2011; Cayirci 2013). Moreover, there are modelling and simulation software offered as cloud service in the Internet. However, to the best of our knowledge, a definition of MSaaS that is agreed by everyone and clarifies the distinction between MSaaS and Software as a Service (SaaS) (Armbrust et al. 2010; Garg, Versteeg, and Buyya 2011; Hwang, Fox, and Dongarra 2011; Valipour et al. 2009; Zhang et al. 2011) is still not available in the literature. At the first glance, it is not easy to see the difference between SaaS and MSaaS, because MSaaS is in essence a special form of SaaS. The inter-relations between MSaaS and conventional cloud services, i.e., SaaS, Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), are depicted in Figure 1.

MSaaS is a model for provisioning M&S services on demand from a cloud service provider (CSP), which keeps the underlying infrastructure, platform and software requirements/details transparent from the users. CSP is responsible for licenses, software upgrades, scaling the infrastructure according to evolving requirements, and accountable to the users for providing grade of service (GoS) and quality of service (QoS) specified in the service level agreements (SLA). We consider three types of MSaaS as illustrated in Figure 1: modelling as a service, model as a service and simulation as a service. Users may use any of these services and store the results for later use in the CSP that provides these services, in another CSP or in their own personal or corporate environment. They may develop models by using modelling as a service, use previously developed models to run simulations in their own environment or run simulations by using simulation as a service from a CSP.

MSaaS has being considered also by militaries (Cayirci 2013) as the approach for the next generation M&S. Several military MSaaS architectures are under development with ambitious timelines, such as, 2019-2020 for deployment. Due to security considerations and policies, all of these MSaaS architectures are being designed as private clouds. They will offer M&S services that can be composed into an MSaaS at a selected abstraction level with a given fidelity and resolution. We expect that these private clouds will also be connected to each other and create partner clouds for alliances, such as North Atlantic Treaty Organization (NATO).

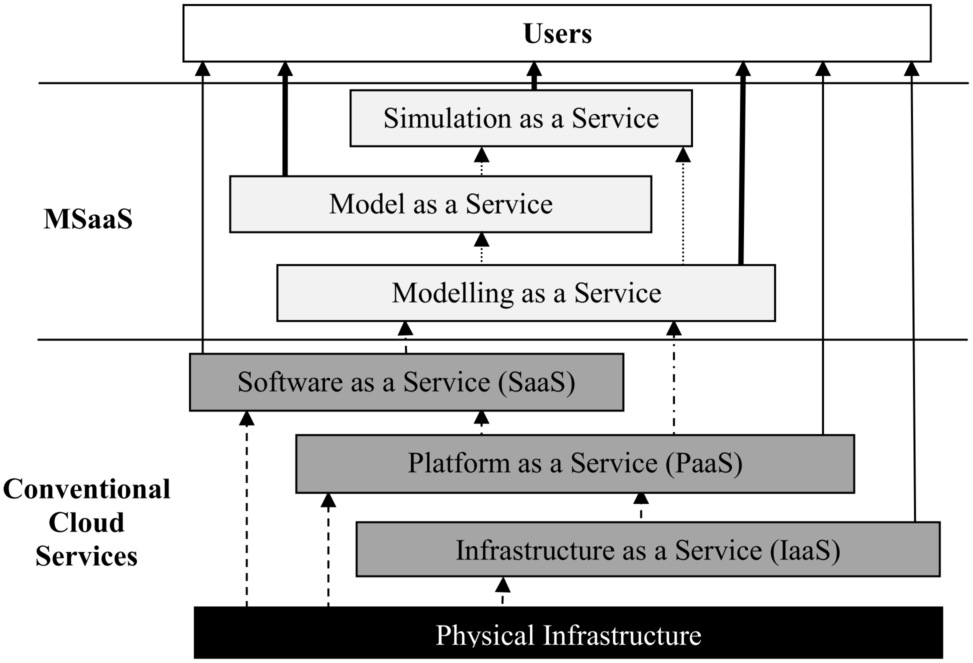

Users
Simulation as a Service
Model as a Service
MSaaS
Modelling as a Service
Software as a Service (SaaS)
Platform as a Service (PaaS)
Conventional Cloud Services
Infrastructure as a Service (IaaS)
Physical Infrastructure

Figure 1: The inter-relations of cloud services including MSaaS

Partner clouds will introduce the need for inter-cloud service federations. Inter-cloud service federations are also frequently named as multi-cloud computing or cloud mash-ups in the cloud computing literature. The term "federation" has a different meaning in cloud computing from the M&S domain. In cloud computing, federates in a federation is not only software entities but also clouds that contribute a federation with infrastructure or platforms, and therefore a federation means an inter-cloud service that integrates various resources in the form of IaaS and PaaS from multiple clouds (Buyya, Ranjan, and Calheiros 2010). When we extend the concept of federation in cloud computing with the meaning of federations in distributed M&S domain, we can categorize MSaaS federations into four broad classes as the following:

- Type 0: Multiple MSaaS in the form of standalone applications located in the same data-center are federated (Toosi et al. 2011).
- Type 1: Multiple service modules located in the same data-center are composed into a composite MSaaS following service oriented architecture (SOA).
- Type 2: Various standalone applications from various data-centers that may belong to different clouds are integrated into a seamless federation by an MSaaS provider (Cayirci 2013).
- Type 3: Not standalone applications, but software modules and data located in multiple data-centers are brought together for dynamically configured service oriented software federations. The data-centers that provide service modules may belong to different clouds (Cayirci 2013).

For any type of MSaaS federation, trust is a key prerequisite. Users need to trust that the provider secures the users' data and information, and provides the quality of service (QoS) and grade of service (GoS) agreed in service level agreements (SLA). Hence, both users and providers take risk. Users' risk is that the security, QoS and GoS agreed in SLA may not be provided, and their operations may be hampered or the security of their data is violated. The providers' risk is two folded: They may not be able to fulfil an SLA, and therefore face penalties and loose reputation. Secondly, a provider may also be a user for the services by the other clouds in an MSaaS federation architecture, and therefore providers are also subject to risk similar to the users'.

In this paper, we focus on partner clouds for MSaaS, and specifically security and trust related challenges in MSaaS partner clouds. We first survey the literature related to risk, accountability and trust in cloud computing in Section 2. Then, we develop a joint trust and risk model for MSaaS federations in Section 3. We provide some numerical evaluations by using our model in Section 4, and conclude our paper in Section 5.

2 RISKS, ACCOUNTABILITY AND TRUST IN CLOUD COMPUTING

Cloud computing services use autonomic mechanisms for self-configuration, self-optimization and self-healing. These mechanisms make decisions on allocating resources (i.e., physical servers, computation power and memory), and migrating data and processes among servers. These decisions are typically based on pre-set policies that can be modified by CSP. Because of this autonomic nature of cloud computing, CSP may not be able to identify exactly in which physical machine data are stored or a process is hosted. In addition to this, multi-tenancy allows multiple users share the same software concurrently. Moreover, a software used by multiple users may process data owned by various users and data may have parts with different classification levels. Therefore, cloud computing introduce new vulnerabilities although it seems providing more secure environment at the first glance (Cayirci 2013). The list of security threats based on the exploitation of these vulnerabilities is long (Cayirci 2013). The security threats that a CSP faces are further exacerbated by the nested cloud architectures. Even private clouds for military may have server farms and data centers in many countries, and may be receiving cloud services from public clouds and linked to some partner clouds.

The increased list of vulnerabilities and security threats exacerbate the risks that a CSP has to take. The literature on risk is extensive with a very large scope of application areas. Therefore, we will not attempt to survey all the literature but refer to (DHS 2008; Ezell et al. 2010; Kaplan and Garrick 1980; Voeller 2010). In the seminal paper by Kaplan and Garrick, the distinctions between uncertainty, hazard and risk are clarified, and the absolute and perceived risk notions are explained. Risk analysis is defined as "an attempt to envision how the future will turn out if a certain course of action or inaction is taken" (Kaplan and Garrick 1981). Three questions are answered during a risk analysis:

- A scenario s_i (i.e., What can go wrong?)
- The probability p_i of s_i (i.e., the probability that the scenario is realized)
- The consequence x_i of s_i

Hence, the risk R is a set of triplets that answers three questions (i.e., $R=\{<s_i, p_i, x_i>\}, i=1, 2, ..., N$) for N scenarios (i.e., N represents the number of all possible scenarios) (Kaplan and Garrick 1981).

The risk that a cloud user has to accept are higher than a CSP. CSP usually keep the locations of their server farms and data centers confidential from users. Additionally, CSP have to prioritize the issues to solve when risks are realized. These uncertainties increase risk (Kaplan and Garrick 1981) and imply that the users have to trust CSP (Rousseau et al. 1998). A user has to rely on the autonomic procedures of CSP for managing the infrastructure appropriately according to the users' security dynamics, treating the users' issues in a timely manner, detecting, recovering and reporting the security incidents accurately. Therefore, CSP have to be accountable to their users, and in many cases the users should be able to transfer their accountability to their CSP. However, since we expect that CSP may use services by the other CSP and even private clouds may be linked to partner clouds, the transfer of accountability may end up at a CSP whose accountability does not mean anything to the end user. It is clear that the nested nature of clouds make accountability an extremely sophisticated issue and increases the risk for users.

Risk, trust and accountability should not be treated as related only to security but also QoS and GoS. The centralization of resources and sharing them increase the utilization. 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 users need to be assured that their 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.

The bottom-line is that accountability (Pearson and Charlesworth 2009) and trust are concepts required to be realized before potential users embrace cloud computing approach. Therefore, "trust" with cloud computing perspective has been extensively studied in the literature recently (Aljazzaf 2012; Pearson 2012; Rashidi and Movahhedinia2012), and "trust as a service" is introduced to cloud business model.

Definition of trust can be a starting point for modeling it. In (Mayer, Davis, and Shoorman 1995) and (Roussaeau 1998), 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 (Pearson 2012). There are also hard and soft aspects of trust (Wang and Lin 2008; Singh and Morley 2009; Osterwalder 2001). 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 (Ryan et al. 2011), the authors introduced not only security but also accountability and auditability as elements which impact user's trust in cloud computing, and can be listed among the hard aspects. In (Kandukiri, Paturi, and Rakshit 2009), Service Level Agreement (SLA) is identified as the only way that the accountability and auditability of a CSP is clarified and therefore a CSP can make users trust them. The conclusion is that "trust" is a complex notion to define.

In (Rashidi and Movahhedinia 2012), the user trust to a CSP is related to the following parameters:

- Data location: Users know where their data are actually located.
- Investigation: Users can investigate the status and location of their data.
- Data segregation: Data of each users are separated from the others.
- Availability: Users can access services and their data pervasively at any time.
- Privileged user access: The privileged users, 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 above the required standards for a long time.

The authors in (Rashidi and Movahhedinia 2012) statistically analyze the results of a questionnaire answered by 72 cloud users to investigate the perception of the users on the importance of the above parameters. According to this analysis, backup and recovery produces strongest impact on user's trust in cloud computing followed by availability, privileged user access, regulatory compliance, long-term viability and data location. Their survey showed that data segregation and investigation have weak impact on user's trust on cloud computing.

Chief information officers perceives the barriers for cloud adoption (Pearson 2012) as vendor lock-in (i.e., to be dependent on a vendor), cloud performance and availability, security and challenges in integrating internal and external services. According to another survey among 264 non information technology executives (non-IT) and 462 information technology executives, the barriers are security, regulatory risks, business case, adapting business processes, interoperability, lack of awareness, adjusting policies and building skill sets (Pearson 2012). These barriers are important in trust modelling because they are why the potential users trust or do not trust a CSP.

3 A TRUST AND RISK MODEL FOR MSAAS FEDERATIONS

As explained in Section 2, trust definition is mainly based on the vulnerability that the trusting party is exposed to by this trust relation, and both positive and negative actions taken against this vulnerability by the trusted party. Such a trust relation has both hard and soft parts and is a very sophisticated notion. In this section, we introduce a practical statistical approach that can be used by a trust as a service (TaaS) or reputation as a service provider. Please note that we do not propose an architecture or mechanism to build trust but a model that can be used for deciding if a service is trustworthy enough to receive. This model can be embedded into an overarching framework such as the one introduced in (Singhal et al. 2013).

In our model, we evaluate risk and trust jointly. The real risk is the risk that cannot be (or is not) eliminated by the CSP. If the part of the security risk δ_s and the service outage risk δ_g not eliminated by the CSP is lower than the user can take τ_s *and* τ_g, then the cloud service is viable for the user. For this equation, we perceive the risk as the probability r_s that a security threat is realized or the probability r_g that a service outage occurred, and trust as the probability t_s that the CSP can eliminate a security threat when realized or the probability t_g that the CSP can recover from a service outage before it hampers the user's operations. Therefore, a TaaS recommends a cloud service if and only if $\delta_s > \tau_s$ and $\delta_g > \tau_g$,where

$$\delta_s = r_s - (r_s \times t_s)\text{, and} \tag{1}$$

$$\delta_g = r_g - (r_g \times t_g)\,. \tag{2}$$

Risks r_s and r_g can be measured by using periodical data weighted based on their freshness as follows:

$$r_{s(i)} = (1-\omega) r_{s(i-1)} + \frac{\omega \varepsilon_i}{u_i}\text{, and} \tag{3}$$

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

Observations for Equations (3) and (4) are made in periods. 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. We examine the sensitivity of our model to the period length in Section 4. The period i is the latest period, and $r_{s(i)}$ and $r_{g(i)}$ are the current risk assessments for security and service outage respectively. The parameter ω is the weight parameter. The number of subscribers subject to at least one security incident and at least one service outage at the last period are ε_i and ρ_i respectively. The total number of subscribers at the last period is u_i.

Trust parameters t_s and t_g, consists of two parts, i.e., hard t_{sh}, t_{gh} and soft t_{ss}, t_{gs}, as shown in Equations (5) and (6):

$$t_s = \begin{cases} 0, & \text{if } t_{sh} + t_{ss} < 0; \\ 1, & \text{if } t_{sh} + t_{ss} > 1; \\ t_{sh} + t_{ss}, & \text{otherwise.} \end{cases} \tag{5}$$

$$t_g = \begin{cases} 0, & \text{if } t_{gh} + t_{gs} < 0; \\ 1, & \text{if } t_{gh} + t_{gs} > 1; \\ t_{gh} + t_{gs}, & \text{otherwise.} \end{cases} \tag{6}$$

Hard trust is measured similar to risk:

$$t_{sh(i)} = (1-\omega)t_{sh(i-1)} + \frac{\omega\varepsilon_{ei}}{\varepsilon_i}. \tag{7}$$

$$t_{gh(i)} = (1-\omega)t_{gh(i-1)} + \frac{\omega\rho_{ri}}{\rho_i}. \tag{8}$$

In Equations (7) and (8), ε_{ei} is the number of subscribers whose all security threats are eliminated without any damage when they are realized at period *i*, and ρ_{ri} is the number of users whose all service outages are recovered from without hampering their operations at period *i*. Soft parts of trust $t_{ss(i)}$ and $t_{gs(i)}$are calculated based on the deviation from the weighted average:

$$d_{s(i)} = t_{sh(i-1)} - \frac{\varepsilon_{ei}}{\varepsilon_i};$$

$$d_{g(i)} = t_{gh(i-1)} - \frac{\rho_{ri}}{\rho_i};$$

$$t_{ss(i)} = \begin{cases} d^{\gamma}_{s(i)}, & \text{if } d_{s(i)} \geq 0; \\ -\sqrt[\gamma]{\left|d_{s(i)}\right|}, & \text{if } d_{s(i)} < 0; \end{cases} \tag{9}$$

$$t_{gs(i)} = \begin{cases} d^{\gamma}_{g(i)}, & \text{if } d_{g(i)} \geq 0; \\ -\sqrt[\gamma]{\left|d_{g(i)}\right|}, & \text{if } d_{g(i)} < 0. \end{cases} \tag{10}$$

In Equations (9) and (10), the slope value γ is to imitate the relation of trust with the negative behavior. If the performance of the CSP gets worse, 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.

Equations (1) and (2) are for single service risk. Since MSaaS federations consists of multiple services, we extend them as follows:

$$S = 1 - \prod_{k=1}^{n}(1-\delta_{sk})\text{; and} \tag{11}$$

$$G = 1 - \prod_{k=1}^{n}(1 - \prod_{m=1}^{a_k}\delta_{gkm}). \tag{12}$$

In Equations (11) and (12), *S* and *G* are the expected (i.e., the risk that cannot be eliminated by the CSP) overall security and service outage risk for MSaaS federations respectively. The number of services in the composed federation is *n*, and a_k is the number of alternative services available for service *k* in the inter-cloud (all the clouds that can be accessed for this service). It is trivial to see at Equation (11) that the higher the number of services compose a federation, the higher the security related risk becomes. The same relation can also be observed at Equation (12) with a difference: the higher number of alternatives decreases the service outage related risk. We examine these relations more detailed in Section 4. Finally, a TaaS recommends a service federation if and only if $S>\tau_s$ and $G>\tau_g$.

4 ANALYSIS

In this section, we analyze the relation of security risk *S* and service outage risk *G* with various parameters through static Monte-Carlo simulations. In Figure 2, the sensitivity of security risk *S* to the changes in the number of federates *n* is depicted. There is a linear relation between *S* and *n*. The relation of service outage risk *G* with the parameters *n* and a_k (i.e., the number of alternative services offered for the same federate) is more sophisticated and depicted in Figure 3. When the average number of alternative services for each federate is more than three, the service outage risk becomes almost zero and independent from the changes in the number of federates. Otherwise, the sensitivity of *G* to *n* is similar to the sensitivity of *S* to *n*.

Both Figures 2 and 3 are for the case that δ_s=0.01 and δ_g=0.02. When δ_s and δ_g are increased for the same number of federates and alternative services, S and G values also increase linearly as illustrated in Figures 4 and 5.

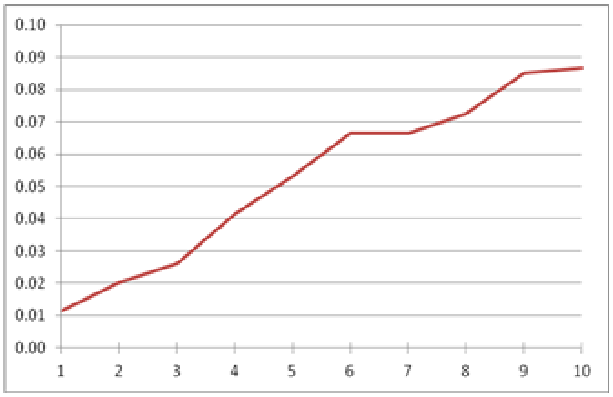


Figure 2: S values for 1-10 federates in a federation when δ_s=0.01

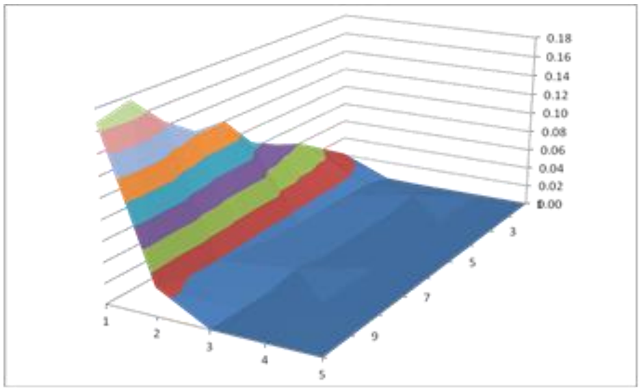


Figure 3: G values for 1-10 federates and 1-5 alternative services for each federate when average δ_s=0.01 and average δ_g=0.02

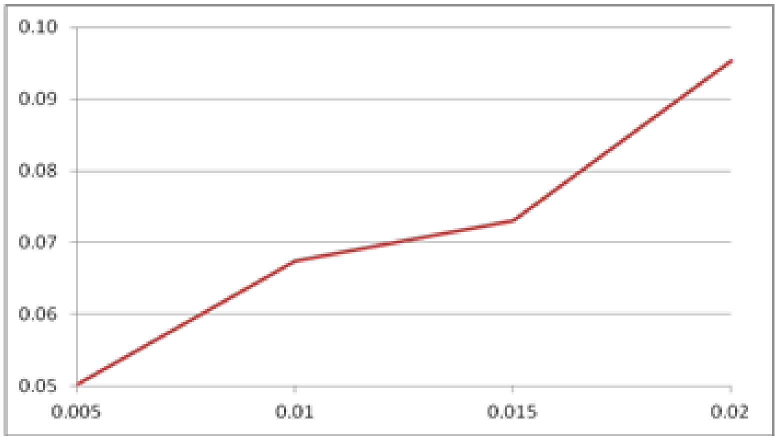


Figure 4: S values for δ_s values between 0.005 and 0.02 and average number of federates is 5

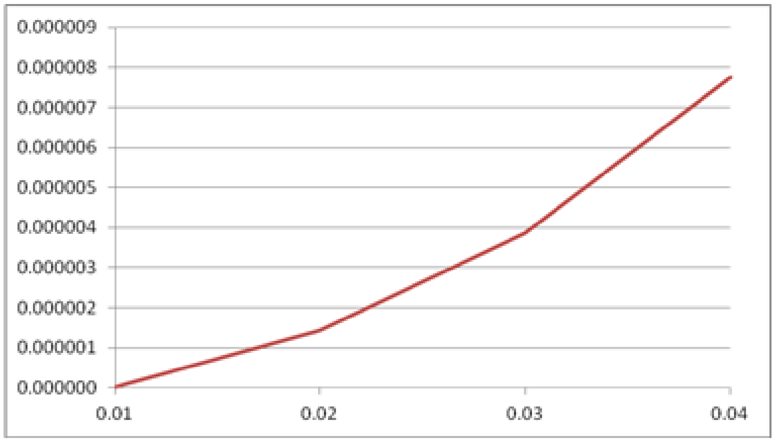
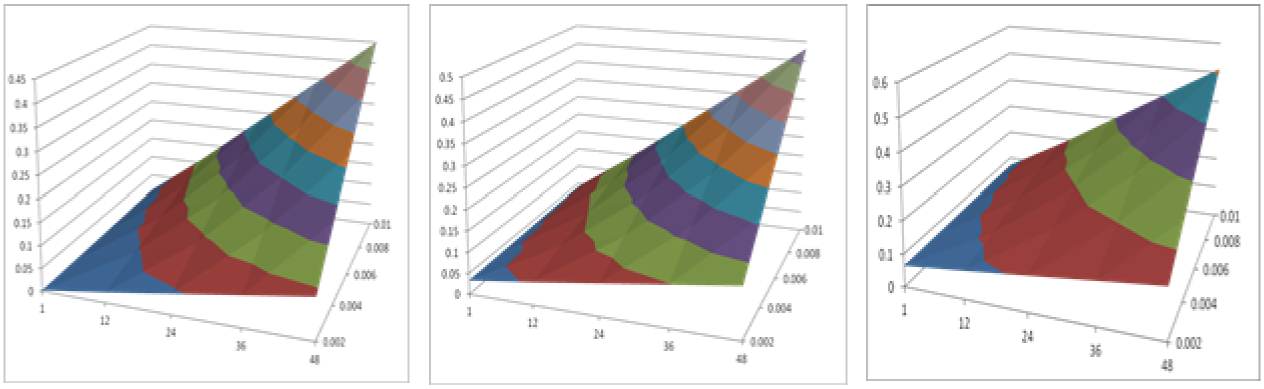


Figure 5: G values for δ_g values between 0.01 and 0.04, average number of federates is 5 and average number of alternative services for each federate is 4

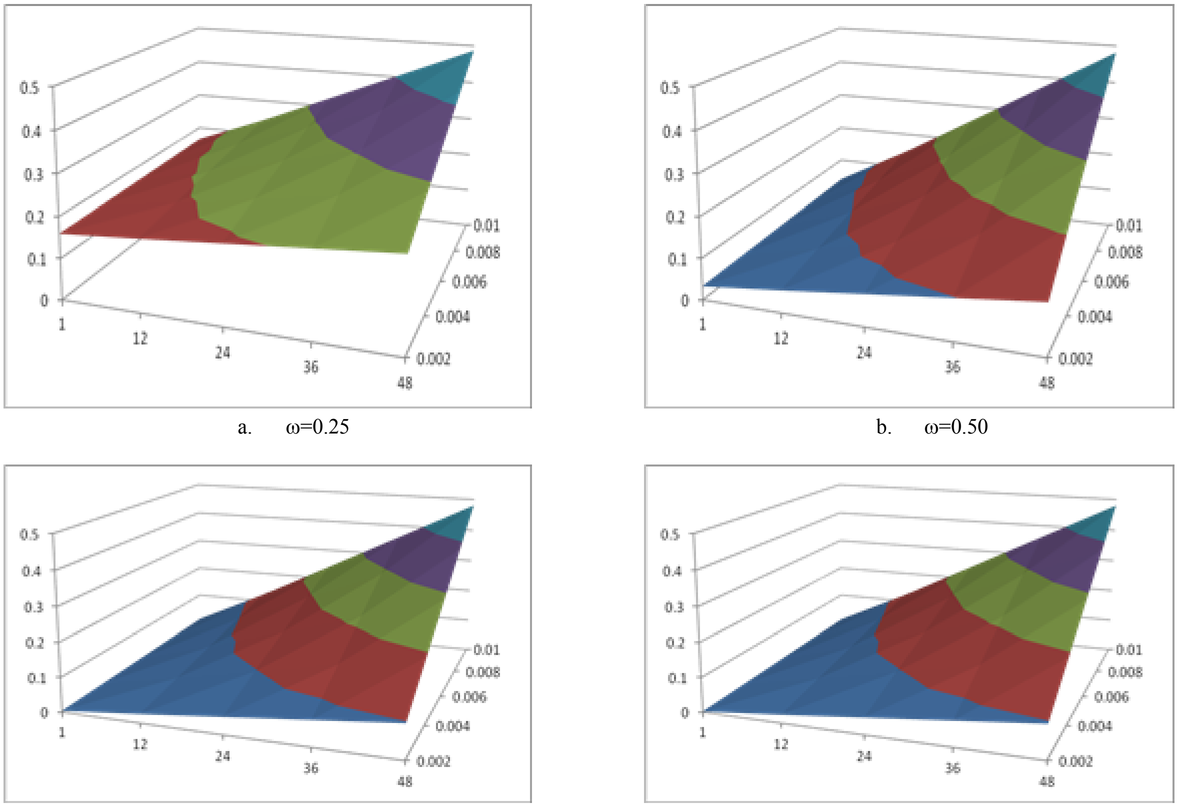
Neither S nor G is sensitive to the changes in the number of users when the expected number of security incidents and service outages are averaged per person respectively. However, the period length and the average rate of security incidents and service outages per person affects S and G as depicted in Figures 6(a) – 6(c).

Figure 6 shows that the initial values assigned to S and G does not make much difference when ω=0.5. Risk assessment converges to more accurate values quite quickly after startup. This is quicker as expected and depicted in Figure 7, when weight value ω is higher. The model produces more optimistic results (i.e., Risk perception gets lower.) when the observation period length is shorter. For one hour period length, the S and G values becomes much less sensitive to the changes in the values assigned to risks r_s and r_g comparing to higher period lengths such as 36 or 48 hours. The same can be observed both in Figures 6 and 7.



a. Initial risk is 0.0 b. Initial risk is 0.5 c. Initial risk is 1.0

Figure 6: Risk (both S and G) estimate after five periods for period lengths between 1 and 48 hours and average period risk between 0.002 and 0.01 when ω=0.5



a. ω=0.25

b. ω=0.50

c. ω=0.75

d. ω=1.00

Figure 7: Risk estimate (both S and G) after five periods for period lengths between 1 and 48 hours and average period risk between 0.002 and 0.01 when initial risk is 0.5

Figure 8 shows the effect of weight parameter *ω* better than Figure 7, because the period length is 1 hour and the same average risk (i.e., δ_s and δ_g) are repeated at every period for the results in Figure 8. Therefore, when the weight parameter *ω* is 1, that represents the most accurate average of all the simulation periods. When the weight parameter *ω* is less than 0.5 and initial risk estimate is 0.5, the risk perception of the model is quite different (i.e., around 0.1) from the real value after the completion of the first 5 periods. Based on this observation, we recommend assigning 1 to the weight parameter ω at the startup, and gradually decreasing it towards the desired weight parameter in every period. When the weight parameter is higher, the model has tendency to forget the previous performance and becomes more reactive to the current performance.

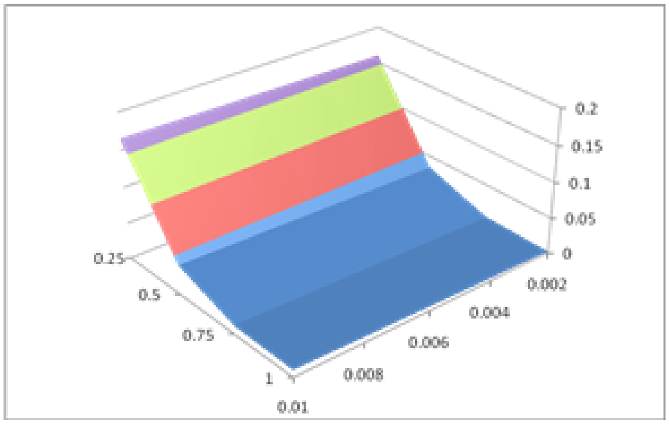


Figure 8: Risk estimate (both S and G) after five periods for ω between 0.25 and 1, and average period risk between 0.002 and 0.01 when initial risk is 0.5 and period length is 1 hour

5 CONCLUSION

Risk, trust and accountability are critical notions for MSaaS 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 MSaaS, trust relation between the subscribers and the CSP has to be established. This requires an in depth understanding of risk and the accountability of the CSP. MSaaS federations, which are basically cloud service mash-ups, exacerbates the complexity of accountability, risk and trust relations among the subscribers and the CSP. Therefore, practical services possibly in the form of TaaS are required. A TaaS 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 addresses not only the security related risk but also the risk related to the performance of the services. It differentiates the negative performance from the positive performance in risk assessment based on the subscribers preferences. It also takes into account the freshness of the data about the performance of the CSP again according to the parameters specified by the users. The model is simple enough to be practical for a TaaS used for MSaaS. Our initial experimentation also shows that its results are aligned with the perception of risks and trust as explained in the literature.

ACKNOWLEDGMENTS

This work was supported by EU FP7 Accountability for Cloud and Other Future Internet Services (A4Cloud) Project.

REFERENCES

Armbrust, M., A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. 2010. "A View of Cloud computing." *Communications of the ACM* 53(4): 50–58.

Buyya, R., R. Ranjan, and R.N. Calheiros. 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)*: 13–31.

Cayirci, E. 2013. “Modelling and Simulation as a Service: A Survey.” In *Proceedings of the 2013 Winter Simulation Conference*, edited by R. Pasupathy, S.-H. Kim, A. Tolk, R. Hill, and M. E. Kuhl, forthcoming. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Cayirci, E., and C. Rong. 2011. “Intercloud for Simulation Federations.” *The Second International Workshop on Cloud Computing Interoperability and Services (Intercloud 2011)*.

DHS. 2008. *DHS Risk Lexicon*. Department of Homeland Security.

Ezell, B.C., S.P.Bennet, D. Von Winterfeldt, J.Sokolowski, and A.J.Collins. 2010. “Probabilistic Risk Analysis and Terrorism Risk.” *Risk Analysis* 30(4): 575-589.

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*.

Hwang, K., G. Fox, and J. Dongarra. 2011. *Distributed and Cloud Computing.* San Francisco: Morgan Kauffmann Publishers.

Kandukuri, B.R., R. Paturi, and V.A. Rakshit. 2009. “Cloud Security Issues.” *IEEE International Conference on Services Computing*.

Kaplan, S., and B.J. Garrick. 1981. “On The Quantitative Definition of Risk.” *Risk Analysis* 1(1): 11-27.

Mayer, R. C., J. H. Davis, and F. D. Schoorman. 1995. “An Integrative Model of Organizational Trust.” *The Academy of Management Review* 20(3): 709–734.

Osterwalder, D. 2001. “Trust Through Evaluation and Certification.” *Social Science Computer Review*. Sage Publications, Inc. 19(1): 32-46.

Pearson, S. 2012. “Privacy, Security and Trust in Cloud Computing.” In *Privacy and Security for Cloud Computting, Computer Communications and Networks,* edited by S. Pearson and G.Yee, 3-42. New York: Springer-Verlag.

Pearson, S., and A. Charlesworth. 2009. “Accountability as a Way Forward for Privacy Protection in the Cloud.” In *Proceedings of the 2009 CloudCom*, edited by M.G. Jaatun, G. Zhao, C. Rong, 131-144. New York: Springer-Verlag.

Rashidi, A., and N. Movahhedinia. 2012. “A Model for User Trust in Cloud Computing.” *International Journal on Cloud Computing: Services and Architecture(IJCCSA)* 2(2):1-8.

Rousseau, D., S. Sitkin, R. Burt, and C. Camerer. 1998. “Not so Different After All: a Cross-discipline View of Trust.” Academy of Management Review 23(3): 393-404.

Ryan, K. L. K., P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee. 2011. “TrustCloud: A Framework for Accountability and Trust in Cloud Computing.” *2nd IEEE Cloud Forum for Practitioners (ICFP)*.

Singh, S., and C. Morley. 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.

Singhal, M., S. Chandrasekhar, G. Tingjian, R., S. Sandhu, R. Krishnan, G-J. Ahn, and E. Bertino. 2013. “Collaboration in Multicloud Computing Environments: Framework and Security Issues.” *IEEE Computer Magazine* 46(2): 76-84.

Toosi, A.N., R.N.Calheiros, R.K.Thulasiram, and R.Buyya. 2011. “Resource Provisioning Policies to Increase IaaS Provider's Profit in a Federated Cloud Environment.” *HPCC 2011*.

Valipour, M.H., B. AmirZafari, K.N.Maleki, and N.Daneshpour. 2009. “A Brief Survey of Software Architecture Concepts and Service Oriented Architecture.” *Proceedings of 2nd IEEE International Conference on Computer Science and Information Technology, ICCSIT'09*: 34-38.

Voeller, J.G. 2010. *Wiley Handbook of Science and Technology for Homeland Security*. New Jersey: Wiley & Sons, ISBN 978-0-470-08792-3.

Wang, Y., and K.-J. Lin. 2008. "Reputation-Oriented Trustworthy Computing in E-Commerce Environments." *Internet Computing* 12(4): 55–59.

Zhang F., J. Cao, K. Hwang, and C. Wu. 2011. "Ordinal Optimized Scheduling of Scientific Workflows in Elastic Compute Clouds." *Third IEEE Int'l Conf. on Cloud Computing Technology and Science*, (CloudCom2011).

AUTHOR BIOGRAPHIES

ERDAL CAYIRCI graduated from Army Academy in 1986 and from Royal Military Academy, Sandhurst in 1989. He received his MS degree from Middle East Technical University, and a PhD from Bogazici University both in computer engineering in 1995 and 2000, respectively. He retired from the Army when he was a colonel in 2005. He was an Associate Professor at Istanbul Technical University, Yeditepe University and Naval Sciences and Engineering Institute between 2001 and 2005. Also in 2001, he was a visiting researcher and lecturer at the School of Electrical and Computer Engineering, Georgia Institute of Technology. He is currently Head, CAX Support Branch in NATO's Joint Warfare Center in Stavanger, Norway, and also a professor in the Electrical Engineering and Computer Science Department of University of Stavanger. His research interests include cloud computing, modelling and simulation, security in ad hoc networks, sensor networks and mobile communications. Professor Cayirci received the "2002 IEEE Communications Society Best Tutorial Paper" Award, the "Fikri Gayret" Award from Turkish Chief of General Staff in 2003, the "Innovation of the Year" Award from Turkish Navy in 2005 and the "Excellence" Award in ITEC 2006. He is author of two textbooks, "Security in Wireless Ad Hoc and Sensor Networks" and "Computer Assisted Exercises: A Reference Guide," both published by John Wiley & Sons. His email is erdal.cayirci@uis.no.