Risk-based Service Selection in Federated Clouds

Usama Ahmed[1], Ioan Petri[2], Omer Rana[3], Imran Raza[1] and Syed Asad Hussain[1]
[1] *Department of Computer Science, COMSATS University Islamabad, Lahore Campus, Pakistan*
[2] *School of Engineering, Cardiff University, UK*
[3] *School of Computer Science & Informatics, Cardiff University, UK*

***Abstract*—The Cloud Service Provider (CSP) marketplace has continued to expand in recent years. Although a few major providers dominate (e.g. AWS, Google Cloud, Microsoft Azure), there are also a number of specialist providers offering hosting services and computing platforms[1]. A single Cloud provider can also offer a marketplace for their own offerings – e.g. the AWS Marketplace[2], which enables third party libraries to be deployed as services within AWS instances. In order to determine whether a particular CSP should be used, clients need to apply preliminary assessment and evaluation when provisioning services on such a provider. Service selection can be realised based on different decision-making criteria, to enable a more informed selection process for clients.** *Trust* **can be utilised as a mechanism to inform such selection decisions. Trust can have different representations and utilise parameters derived from past interactions. Trust therefore represents an** *expression of risk* **associated with a service exchange between clients and providers. We present a trust-based risk evaluation for CSP selection in federated clouds, with a particular focus on security & data privacy. We use a scenario from an Architecture, Engineering & Construction (AEC) project to demonstrate how such a selection can be made, and is of benefit in developing the federated system. A methodology for the selection process is outlined, making use of metrics and certification processes from the Cloud Security Alliance (CSA). The proposed approach can also be generalised to other application domains with similar requirements.**

1. Introduction

Combining capability & capacity from multiple Cloud Service Providers (CSPs) is a common requirement across many industry projects. Understanding when and how capability (both infrastructure and services) can be combined across multiple (independent) providers enables: (i) aggregation of services that are difficult to provision locally by one CSP; (ii) access to computing infrastructure (storage, compute) that can be used on-demand; (iii) cost efficiency in using and releasing infrastructure on-demand. However, determining which CSP to include within a federation remains a challenge, particularly when multiple CSPs are available offering similar capabilities. Federation of cloud systems has provided a common framework for providers to exchange data and collaborate by connecting their local infrastructure. The supporting mechanisms for cloud federation can bring considerable value for clients by offering them low cost access to global services which otherwise induces higher costs for establishing new infrastructure (which is needed for peak workloads over short time frames and remains unused for most of the time).A federated cloud also allows users to host applications with cloud provider of their choice. This enables users to make local decisions about software libraries/ systems, pricing and deployment environments, while still remaining connected to other computational resources. Through federation, it is also possible for an organization to run specific parts of their business functions on different platforms, e.g. ERM, Human Resources, Marketing etc can each be hosted on independently managed CSPs (including in-house systems). Numerous cloud bridging solutions now exist in market, like IBM's Cast Iron Cloud Integration [1], which is a part of Web Sphere suite of tools used across various environments in development and deployment of applications. Though the use of different plugins, Cast Iron enables integration with a number of IBM products (such as DB2) and systems from different vendors, such as SAP and Salesforces CRM – hence enabling an integration between in-house systems and public and private Cloud environments [3]. Similar *bridging* platforms are also available from other vendors, e.g. Oracle Cloud Machine (which can be hosted at customer premises and which can be connected to an external data center). However, a lot of these systems are proprietary to their respective vendors. For this reason these systems are quite inflexible to be customised for a particular use-case scenario. CometCloud [4] is an open source solution that has its validation from working in numerous financial and scientific scenarios. CometCloud has proven to work along specialist computing environments (such as in case of large scale compute clusters within US TeraGrid and XSEDE projects) and public Cloud systems from Amazon. (described in section 1.1) [2].

1.1. Cloud Bridging & Federation

In construction projects, numerous companies are brought together to collaborate over the life-cycle of the

[1] CloudHarmony reports 90 providers: https://cloudharmony.com/directory

[2] https://aws.amazon.com/marketplace

building construction using different systems and storage solutions. As part of this collaboration, access control, authorization and privacy of various data objects created during the entire life-cycle is critical to the successful realization of the project along with their compatibility. Currently, coordination between collaborators is a rigorous manual procedure and requires a monopoly of software systems to be enforced. In this work we consider a case study of Clouds-4-Coordination system, a federated cross-cloud space that has been built for coordination among multi-site construction projects through the use of Virtual Enterprise (VE) concept. Recently, the projects in Architecture/Engineering/Construction (AEC) industry are increasingly being undertaken by consortia of companies and individuals that collaboratively work for the entire project duration. Such kind of projects are inherently complex and its participants have to put different levels of skill to use in the project from its beginning to the end. In the meanwhile, different data artifacts are also produced which needs to be stored and shared between these participants.

We describe the use of a Cooperation Threshold Estimation (CTE) when using a new CSP in a collaborative project, illustrated using a scenario in the *Clouds-4-Coordination* federated cloud system. CTE for a project in any given context is based on: i) perceived risk; ii) perceived competence, at a point in time or over a time window; and iii) Importance attached to collaborating. These parameters influence the choice of using an external CSP, comparing the risk vs. benefits in the context of a particular capability (e.g. access to storage, execution of a particular service instance, etc). The rest of the paper is organized as follows. In Section 2, the requirements for trust based selection are discussed. In Section 3, the cooperative threshold estimation is presented. Methodology is presented in Section 4, and the trust evaluation in Section 5. Conclusions are presented in Section 6.

2. Trust-based Provider Selection

Trust is a complex phenomenon and has always been investigated in varying contexts for various application domains and research disciplines [5], [6]. There have been many definitions of trust, notably in the context of philosophy [10], sociology [7], [8], [9], , psychology [12], [13] economics [11] and organizational management [15] etc. However, trust in an entity has always been used as a decision-making measure, and as a method to measure the extent to which an entity (e.g. a CSP) will behave as expected. As a foundation of our proposed research, trust is a factor of: (i) Expectation: the trustee is going to present a specific behavior in a certain way; (ii) Belief: the likelihood at which the expected behavior is certain to occur, as evident from the trustees (past) performance; (iii) Risk: that belief in trustee is worth a risk for some specific purpose. Given a Cloud Service Provider (CSP) x the trust T is the result of expectation resulting from its positive 'ρ' or negative 'η' behavior with a certainty $'c'$ and initial expectation $'a'$, and is given by: $T = \rho + (1 - c) \times a$, where '$\rho$', '$\eta$', c and a are the result of attribute assessment and verification offered by a CSP. Trust can be calculated using a variety of different performance and operational metrics. Based on requirements of AEC projects, where security and data privacy are often key requirements within a consortium, in this work we base this trust assessment on "Security, Trust and Assurance Registry" (STAR) program by the Cloud Security Alliance (CSA). The STAR program is used to support different levels of assessment and certification of CSPs, to enable Cloud Service Users (CSUs) make informed assessment of CSP security capability and maturity.

2.1. Cloud Security Alliance (CSA) STAR Program

The Cloud Security Alliance (CSA) has proposed a "Security, Trust & Assurance Registry (STAR)" program [16] aiming to increase transparency in an attribute-based assessment of CSPs. As a part of this program, the Consensus Assessment Initiative Questionnaire (CAIQ) is provided for CSPs to offer security control transparency. CSA STAR offers a three level assessment and certification program with a free publicly accessible STAR database containing assessment data for more than 200 CSPs.

At the first level, CSPs publish self-assessments of their security controls, in CAIQ format, which is built upon the Cloud Control Matrix (CCM) framework. This self assessment may afterwards be followed by an independent third party audit for security control attestation and certification of a CSP at level two. The third level for continuous monitoring based certification is currently under development [16], ensuring that the assessment can be made on a continuous basis. CSA STAR continuous monitoring enables automation of current security practices, requiring CSPs to publish their security practices according to CSA specifications. Customers and tool vendors can then retrieve and analyse this data for use in a variety of contexts.

2.2. Cloud Control Matrix (CCM) & Consensus Assessments Initiative Questionnaire (CAIQ)

The Cloud Security Alliance CCM provides a control framework for assessing security capability, providing guidance across 16 domains. These controls enable CSPs to report on their security capability in a way that can be attested (verified) by external organisations, using a series of questions that are captured in the CAIQ. The foundations of CCM also relate to other industry-accepted security standards and control frameworks, e.g. ISO 27001/27002, ISACA, COBIT, PCI, NIST, Jericho Forum and NERC CIP. As a framework, the CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry. Cloud providers can use the CAIQ to outline their security capabilities to customers, publicly or privately, in a standardized way. However, the information offered is a CSP's self -assessment; cloud users may want assessments performed by some independent third-party organization.

2.3. Clouds-4-Coordination federation

In the Cloud-4-Coordination context multiple organizations participate to the realization of a construction project. A construction project is a complicated activity usually involving multiple diverse professions and organizations. These organizations range from Small and Medium Enterprises (SMEs) to large multinational corporations. These organizations usually participate in the construction project for different timeframes, and in the meanwhile, they contribute variable amounts and types of data, or sometimes no data at all, to the project. In such a context, the federation is used to enable collaboration between designers, suppliers and facilities managers for a range of design and construction tasks. Each of these disciplines join the project framework (realised using the CometCloud system) by sharing their data from their own data center or cloud.

They key challenge in the Clouds-4-Coordination project is the creation and management of the federation space through CometCloud, where discipline specific service providers can join and leave at any moment of time during the project lifetime without any preliminary evaluation (i.e. assessment of their trust). The process of enabling a new discipline to join the federation has risks implications which need to be mitigated in order to prevent project failure. This is achieved by using a trust-based risk assessment, where each discipline service provider is evaluated based on a "'Cooperation Threshold Estimation" (CTE) to determine the extent to which a discipline service provider can join a project and the benefits it can offer.

In the Clouds-4-Coordination federation, we consider that each site participating in the project must support a local cloud environment. Each discipline has a CometCloud deployment with one master (agent) and several workers, where masters receive project tasks from other disciplines and workers execute tasks and return results to local masters. Each master locally hosts a project model formed of Industry Foundation Classes (IFC) objects, a data format used in the engineering and construction sector. The coordination mechanism in the Clouds-4-Coordination system is based on propagating events to the relevant discipline, i.e. disciplines participating in the project are notified when a new project is created. When a project creation notification is circulated, a master retrieves and updates the project and then creates a new version of the project on the local cloud. The entire federation is managed by a "Federation Manager" (FedMgr) which is in fact the owner of the project (i.e. client), identifying the organization that creates the project and which can always retrieve the latest version of the project.

A key stage of the Clouds-4-Coordination process is when a new discipline is added to the project and to the federation. Here, the $FedMgr$ (coordinator) starts the trust evaluation of the new discipline and evaluates the 'Cooperation Threshold Estimation' metric. The methodology employed for trust based evaluation and selection is presented in Section 3 and Section 4.

3. Cooperation Threshold Estimation

The Cooperation Threshold Estimation (CTE) approach is used to determine the extent to which a CSP x is useful to the Project 'α' in a given context c. Anticipated project Cooperation Threshold (CT), as evaluated by $FedMgr$, is given by:

$$CT(x,\alpha,c) = \sum_{i}^{c}\left(\frac{Perceived\ Risk(x,\alpha,c)}{Perceived\ Competence(x,c) + T(x,c)} \times I(x,\alpha,c)\right) \tag{1}$$

Where $Perceived\ Risk(x,\alpha,c)$ is the overall risk assessment by a client, Perceived Competence (PC) is based on performance metrics of the given CSP 'x'. This PC is calculated by $FedMgr$ along with $T(x,c)$ as being an aggregate result of any previous competence evaluations, if any, thus formulating a 'CSP Profile'. In the above equation $I(x,\alpha,c)$ is the importance of collaboration as anticipated by the disciplines participating in the project $'\alpha'$ in a given context 'c'. The above equation also holds true in case of no context or a generic context involving all perspectives of collaboration.

3.1. Entities

A number of entities as illustrated in Figure 1 are involved in our proposed CTE approach for multi-site construction projects employing cloud federation:

AEC Organizations: An AEC project is a complicated activity usually involving multiple diverse professions and firms (such as architects, engineering, structural, mechanical, electrical, facilities management etc.). These firms range from small companies offering specialist expertise to large multinational companies offering multiple expertise. Each one of these organization will participate in a particular project for a varying time period and, in that time period, will contribute different quantities and types of data to the project. This data may be hosted within an a private Cloud, or in some instances, capacity from a multiple Cloud provider may be used. Increasingly, multiple data sources/ locations are involved, requiring support for merging and federation of data sets (representing different parts of a Building Information Model (realised as IFC classes)). This is the key focus of the Cloud-4-Coordination project, which enables such federation to be realized using the CometCloud system.

$FedMgr$: this is a *trust-aware* discipline that acts as an overall coordinator for a project. It is responsible for starting the federation process across the various data sources that are involved in the project. This entity also implements the CTE approach and uses data from multiple CSPs involved. If a new CSP is to be included in the federation, it has to be confirmed by the $FedMgr$.

Certification sources (Cloud Security Alliance / ENISA): Recommendations and strategies from Cloud Security

Alliance (CSA) and the European Network and Information Security Agency (ENISA) are included and used as a part of this research. CSA offers the CAIQ/CCM framework for cloud security assessment, auditing and certification as a program named CSA STAR mentioned in section 2.2. ENISA offer risk assessment mechanism and strategies for cloud users and businesses that wants to opt for cloud computing solutions for their organizations.

Project User: this refers to the entity responsible for either: (i) identifying the requirements for the project (i.e. the types of capabilities that need to be supported); (ii) carrying out operational management of the AEC project; (iii) managing interactions across the various entities involve in an AEC project.

4. Methodology

The $FedMgr$ (described in section 3.1) is responsible for calculating the CTE score, and illustrated in Figure 1. To become eligible for participating in the federation, a CSP must possess a valid set of CAIQ assessments, based on criteria identified by CSA, along with requisite certification on these criteria. A one-time event at the start of its participation is to provide its CAIQ assessment to the $FedMgr$. This CAIQ assessment is parsed by the Trust Representation process to get trust metric required by Trust Evaluation function. The Trust Evaluation function is responsible to evaluate a numerical representation of the competence of the given CSP and to store the same in repository to further evaluate the Cooperation Threshold. As further illustrated in Figure 1, the project owner, whether an individual or an organization, is responsible for initiating the start of federation. Afterwards, more disciplines are added to the shared Project Collaboration Space (PCS) based on their Cooperation Threshold as estimated by the $FedMgr$. Whenever there is a requirement to add a new discipline to the project, an $add\ new\ discipline$ request is forwarded to the $FedMgr$, with the requisite $trust\ criteria$. A list of qualifying CSPs matching this criteria is forwarded to the PCS, where further action regarding the final selection of CSP can be taken according to the project profile. Any CSP x selected from this list is forwarded to $FedMgr$ which in turn initiates the requisite process to engage the given CSP with the federation.

4.1. CSP Profiling

A CSP profile is a consolidated view of the trust and competence of a given CSP registered with the $FedMgr$. Initially, when a CSP joins the federation and has no performance history available, its profile is only based on a *perceived risk* as a result of CAIQ assessment and the level of certification achieved by the CSP collectively known as its *trust posture*:

$$perceived\ risk \propto \frac{1}{trust\ posture}; \tag{2}$$

Hence, trust posture reflects a CSPs ability to conform to Cloud Security Alliance certification and must always be specific to the context of a collaboration. For example, engaging a particular CSP in the federation as a storage repository requres that this CSP only be evaluated from CAIQ controls relevant to storage, instead of all controls. In this way, we can limit CAIQ controls that are relevant for this specific service provision.

4.2. CSP Trust Posture

Our proposed method provides fine-grained and context specific trust values based on CAIQ and CCM by CSA. For trust evaluation, each control domain in CAIQ is represented as an opinion of CSP towards its security practices and is modeled as a subjective belief (beta distribution and Dempster-Shafer belief theory [19]). This opinion is a collective view of CSPs positive and negative answers to assertions of CAIQ hence known as declaration. Considering a generic context in which no domain specification is provided for a collaboration, given p, q, un and NA as the total number of positive, negative, unanswered and not applicable declarations respectively and $N = (p + q + un)$ as the total number of declarations that are applicable in any given context, the trust of a CSP can be evaluated as:

$$T(\lambda, \gamma, \varphi, \epsilon) = \lambda + \varphi * \epsilon \tag{3}$$

given

$$\lambda = \rho * \zeta; \gamma = \eta * \zeta; \varphi = 1 - \zeta; \tag{4}$$

$$\rho = \frac{p}{p+q}; \eta = \frac{q}{p+q}; \zeta = \frac{N * (p+q)}{2 * (N - p - q) + N * (p+q)}; \tag{5}$$

In (5) λ is the belief, γ is the disbelief and φ is the uncertainty of the behavior associated with a CSP. ρ is the average positiveness and η is the average negativeness of a security domain observed from CSA data. Both ρ and η are calculated on the basis of p and q for each domain. A control domain is said to have zero trust value given $p + q = 0$. Confidence, ζ, is calculated based on N, p and q, given $N = (p + q + un)$ and initial expectation $\epsilon = 0.99$ for optimistic scenarios. The overall trust T of a CSP is the average opinion of all domains selected for any given transaction.

TABLE 1. INDIVIDUAL TRUST REPRESENTATION OF FIVE CSPS

CSP	N	p	q	un	λ	γ	φ	T
S	272	228	44	0	0.8382	0.1618	0	0.8864
A	290	208	82	0	0.7172	0.2828	0	0.7172
B	295	211	31	53	0.8706	0.1279	0.0015	0.8721
C	257	110	85	62	0.5627	0.4348	0.0025	0.5652
Q	251	202	22	27	0.9009	0.0981	0.0010	0.9019

In order to elaborate the concept, consider CSPs S, A, B, C and Q having N, p, q and un as specified in Table 1. This data regarding N, p, q and un is the result of numerical representation the CAIQ information of five random CSPs from the CSA STAR database. The values associated with p and q corresponds to the total number of positive and

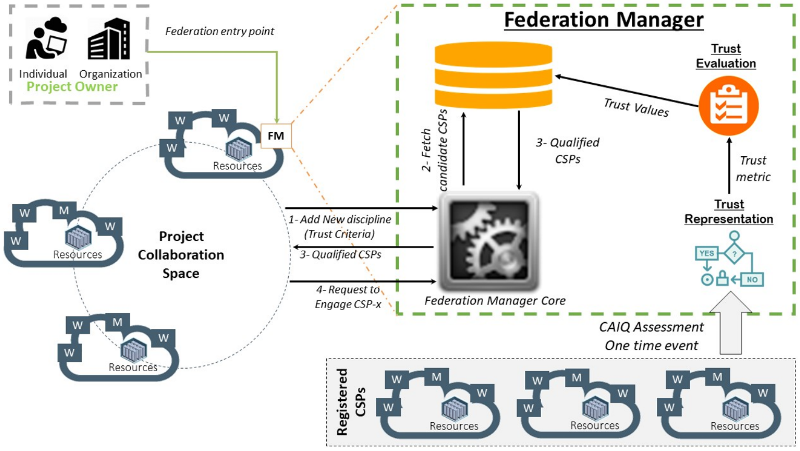

Figure 1. Cooperation Threshold Estimation Methodology

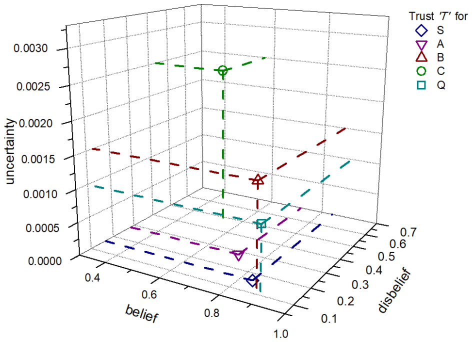

Figure 2. Representation of individual trust values of CSPs

negative assertions that these CSPs have answered. The numbers relating to un are those assertions that were left unanwsered by the CSPs. Afterwards, these three values are aggregated as the total number of applicable assertions N. A three dimensional graphical illustration of these trust parameters for individual CSPs is presented in Figure 2. Belief is represented on X-axis, disbelief on Y-axis and uncertainty on Z-axis. Among these representative CSPs, Q is top rated as having the maximum trust value.

5. Context specific trust evaluation

The relationship between CCM and CAIQ can be used to evaluate trust based on two different types of contexts as given below.

Business context:. A seperation of CAIQ assessment on the basis of control domains. There are a total of 16 control domains as defined in CCM and illustrated in Table 2. Each control domain has its respective number of controls and control assertions. This information allows the trust management system to deliver a context specific trust evaluation when a CSP is interested in providing declarations to fewer control assertions.

TABLE 2. Numerical representation of assertions

No.	ID	Control Domain (16)	Controls (133)	Assertions (295)
1	AIS	Application & Interface Security	4	9
2	AAC	Audit Assurance & Compliance	3	13
3	BCR	Business Continuity Management & Operational Resilience	11	22
4	CCC	Change Control & Configuration Management	5	10
5	DSI	Data Security & Information Lifecycle Management	7	17
6	DCS	Datacenter Security	9	11
7	EKM	Encryption & Key Management	4	14
8	GRM	Governance and Risk Management	11	22
9	HRS	Human Resources	11	24
10	IAM	Identity & Access Management	13	40
11	IVS	Infrastructure & Virtualization Security	13	33
12	IPY	Interoperability & Portability	5	8
13	MOS	Mobile Security	20	29
14	SEF	Security Incident Management, E-Discovery, & Cloud Forensics	5	13
15	STA	Supply Chain Management, Transparency, and Accountability	9	20
16	TVM	Threat and Vulnerability Management	3	10

For example, consider that the stakeholders for a specific project are only interested in AIS, AAC, GRM, IAM and STA control domains. For a CSP x registered with CSA STAR repository and willing to join the federation the complete phenomena of trust posture derivation is depicted in Table 3.

TABLE 3. Numerical representation of assertions

	N	p	q	un	ρ	η	c	λ	γ	ϕ	T	compliance scale
AIS	9	5	4	0	0.5556	0.4444	1	0.5556	0.4444	0	0.5556	No
AAC	13	10	3	0	0.7692	0.2308	1	0.7692	0.2308	0	0.7692	Sufficient
GRM	22	19	3	0	0.8636	0.1364	1	0.8636	0.1364	0	0.8636	Full
IAM	40	25	15	0	0.625	0.375	1	0.625	0.375	0	0.625	Critical
STA	20	20	0	0	1	0	1	1	0	0	1	Full
Aggregate	104	79	25	0	0.7627	0.2373	1	0.7627	0.2373	0	0.7627	Sufficient

As given in Table 3, the trust values for a CSP based on a given context can be evaluated from the assertions relating only to applicable controls. These values in Table 3 are also a result of representing CAIQ information of a random CSP from CSA STAR database. Considering an applicable control GRM from the above example and referring to Table 2, the total number of assertions in the GRM domain are 22, out of which the CSP has positive and negative declarations of 19 and 3 respectively. The overall trust values T of any given domain is shown to be converted to a compliance scale that may be derived from the risk analysis of the project done by the stakeholders (in this scenario, these are other disciplines involved in the project). For example, the compliance of CSP x as in Table 3 is based on a scale with a baseline trust of 0.6, giving us a critical threshold value of 0.6-0.7, Sufficient 0.7-0.8 and Full compliance of 0.8-1.0. In case of qualifying CSPs being more than one, with trust values greater than a given threshold, a comparison is to be made on the basis of similar control domains and compliance scale. Afterwards the trust posture of the given CSP is function of aggregated compliance and the certification level as given by CSA.

The mapping of CCM and CAIQ gives us the number of controls and assertions applicable in case of any given resource, and can be considered in a specific context or for all capabilities of a cloud provider. For example, considering a project requiring storage for its consumers, the only controls and assertion applicable in such a case can be observed from Table 4 i.e. 89 and 253 out of a total of 133 controls and 295 assertions. The applicable assertions are evaluated for trust the same way as mentioned in the above section.

TABLE 4. NUMERICAL REPRESENTATION OF ASSERTIONS

Cont ID.	P(158)	N(194)	C(226)	S(253)	A(240)	D(225)
AIS	2	4	9	9	9	9
AAC	13	13	13	13	13	13
BCR	16	15	17	12	16	17
CCC	2	1	10	17	10	9
DSI	0	2	14	15	15	17
DCS	11	4	4	10	3	3
EKM	0	10	4	15	10	14
GRM	10	10	9	5	12	12
HRS	17	14	14	14	19	22
IAM	20	33	37	12	38	28
IVS	23	29	33	14	25	28
IPY	2	8	4	37	6	6
MOS	9	8	15	28	21	12
SEF	13	13	13	6	13	13
STA	20	20	20	5	20	20
TVM	0	10	10	13	10	2

Whereas in Table 4, P, N, C, S, A and D, refers to Physical, Network, Compute, Storage, Application and Data respectively as given by CCM. Given that a project is in need of more than one type of resource but not all, we may use an OR relationship. Conversely, in strict cases this relationship may change to AND relationship between assertions i.e. all required resources must qualify for compliance in matching controls. A similar method for trust evaluation in resource context is used as described for the business context.

6. Conclusions

Trust based risk assessment in federated clouds can limit *provider lock-in*, and enable access to a variety of different CSPs. This is a key requirement for establishing and sustaining a Cloud marketplace, enabling a range of different platforms and service providers to co-exist. We demonstrate how such trust evaluation can be realized based on (i) perceived risk; (ii) perceived competence, and the (iii) importance of engaging in collaboration. We present the findings of our study in the context of an existing Clouds-4-Coordination project (focusing on Civil Engineering/AEC sector), where the overall assessment of trust can have significant cost implications for a project. Determining risk associated with a provider as a perceived risk can inform the process of provider selection and can prevent possible delays in a project. The certification process used by Cloud Security Alliance is used as a basis for establishing ”trust” and used to determine whether a new CSP should be included within a Cloud federation. We conduct our evaluation by utilizing trust representation from five domains (as identified by Cloud Security Alliance) and emphasize what criterion are relevant when using trust to inform risk assessment of service providers.

References

[1] Solution, IBM CastIron. Last accesed May 21, 2016, https://www-01.ibm.com/software/integration/cast-iron-cloud-integration/salesforce-integration/.

[2] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M., 2010. A view of cloud computing. Communications of the ACM, 53(4), pp.50-58, http://dx.doi.org/ 10.1145/1721654.1721672

[3] Mell, Peter, and Tim Grance. ”The NIST definition of cloud computing.” (2011).

[4] H. Kim and Parashar, M., CometCloud: An Autonomic Cloud Engine, in Cloud Computing: Principles and Paradigms, John Wiley & Sons, 2011, pp. 275-297, http://dx.doi.org/10.1002/9780470940105.ch10.

[5] I. Markov and A. Gillespie, Trust and distrust: Sociocultural perspectives: IAP, 2007.

[6] D. E. Denning, ”A new paradigm for trusted systems,” in Proceedings on the 1992-1993 workshop on New security paradigms, 1993, pp. 36-41.

[7] D. Gambetta, ”Can We Trust Trust?,” 1988.

[8] Y. Yamamoto, ”A morality based on trust: Some reflections on Japanese morality,” Philosophy East and West, vol. 40, pp. 451-469, 1990.

[9] N. Luhmann, ”Trust and power. 1979,” John Willey & Sons, 1979.

[10] B. Barber, ”The logic and limits of trust,” 1983.

[11] B. Lahno, ”Olli lagerspetz: Trust. The tacit demand,” Ethical Theory and Moral Practice, vol. 2, pp. 433-435, 1999.

[12] H. S. James Jr, ”The trust paradox: a survey of economic inquiries into the nature of trust and trustworthiness,” Journal of Economic Behavior & Organization, vol. 47, pp. 291-307, 2002.

[13] J. B. Rotter, ”Interpersonal trust, trustworthiness, and gullibility,” American psychologist, vol. 35, p. 1, 1980.

[14] M. Deutsch, ”Cooperation and trust: Some theoretical notes,” 1962.

[15] R. C. Mayer, J. H. Davis, and F. D. Schoorman, ”An integrative model of organizational trust,” Academy of management review, vol. 20, pp. 709-734, 1995.

[16] cloudsa, ”CSA Security, Trust & Assurance Registry (STAR) - Cloud Security Alliance,” Accessed: 12-Sept-2018, https://cloudsecurityalliance.org/star/overview, 2018.

[17] T. H. Beach, O. F. Rana, Y. Rezgui, and M. Parashar, ”Cloud computing for the architecture, engineering & construction sector: requirements, prototype & experience,” Journal of Cloud Computing: Advances, Systems and Applications, vol. 2, p. 8, 2013.

[18] A. Redmond, A. Hore, M. Alshawi, and R. West, ”Exploring how information exchanges can be enhanced through Cloud BIM,” Automation in construction, vol. 24, pp. 175-183, 2012.

[19] A. Josang, ”The right type of trust for distributed systems,” in Proceedings of the 1996 workshop on New security paradigms, 1996, pp. 119-131.