# Federating Cloud Systems for Collaborative Construction and Engineering

**USAMA AHMED** [1,4], **IOAN PETRI** [2], (Member, IEEE), **OMER RANA** [3], (Member, IEEE),
**IMRAN RAZA** [1], (Member, IEEE), **AND SYED ASAD HUSSAIN** [1], (Member, IEEE)

[1] Department of Computer Science , COMSATS University Islamabad, Lahore Campus 54000, Pakistan
[2] School of Engineering, Cardiff University, Cardiff CF24 3AA, U.K.
[3] School of Computer Science and Informatics, Cardiff University, Cardiff CF24 3AA, U.K.
[4] Department of Software Engineering, Government College University Faisalabad, Faisalabad 38000, Pakistan

Corresponding author: Usama Ahmed (usamaahmed@gcuf.edu.pk)

**ABSTRACT** The construction industry has undergone a transformation in the use of data to drive its processes and outcomes, especially with the use of Building Information Modelling (BIM). In particular, project collaboration in the construction industry can involve multiple stakeholders (architects, engineers, consultants) that exchange data at different project stages. Therefore, the use of Cloud computing in construction projects has continued to increase, primarily due to the ease of access, availability and scalability in data storage and analysis available through such platforms. Federation of cloud systems can provide greater flexibility in choosing a Cloud provider, enabling different members of the construction project to select a provider based on their cost to benefit requirements. When multiple construction disciplines collaborate online, the risk associated with project failure increases as the capability of a provider to deliver on the project cannot be assessed apriori. In such uncontrolled industrial environments, ''trust'' can be an efficacious mechanism for more informed decision making adaptive to the evolving nature of such multi-organisation dynamic collaborations in construction. This paper presents a trust based Cooperation Value Estimation (CoVE) approach to enable and sustain collaboration among disciplines in construction projects mainly focusing on data privacy, security and performance. The proposed approach is demonstrated with data and processes from a real highway bridge construction project describing the entire selection process of a cloud provider. The selection process uses the audit and assessment process of the Cloud Security Alliance (CSA) and real world performance data from the construction industry workloads. Other application domains can also make use of this proposed approach by adapting it to their respective specifications. Experimental evaluation has shown that the proposed approach ensures on-time completion of projects and enhanced collaboration performance.

**INDEX TERMS** BIM, cloud federation, collaboration, construction, trust.

## I. INTRODUCTION

Construction project collaboration supported through hybrid cloud systems can pave the way for real-time multi-disciplinary data exchanges, leading to reduced time [1] for project completion and lower costs [2]. The collaboration between clients, designers, suppliers and facilities managers can involve a range of design and construction tasks, carried out through the use of electronic services [3]. A user or organisation deploying or using a cloud system can take local

The associate editor coordinating the review of this manuscript and approving it for publication was Jing Bi.

decisions about software libraries, deployment environments and pricing while using various platforms to run different portions of their business functions. For example, an organization can host each one of their Enterprise Resource Management, Human Resources and Marketing etc. on independently managed cloud platforms.

In the construction industry, collaborative work on a particular project can give rise to several issues that can cause concern and anxiety for administrators – with much research in recent years being directed towards such challenges [4]–[7]. The issue of trust and ownership in particular has been reported to be most significant for construction

stakeholders [8], [9]. The research literature across the fields of psychology, economics, sociology, and organizational sciences focus on trust in the context of both intra- and inter-organizational collaboration [10]. Another concept closely related to the notion of trust is the occurrence of risk in a construction project [11]. Risk may involve an inadvertent or deliberate act to jeopardize the performance of collaboration or simply not deliver a task that is stipulated as required. The existence of trust when seen as a mechanism to induce confidence, reduces the risk of such opportunistic behavior [12].

This research supports the above mentioned arguments by presenting a scenario of CometCloud [13] based Clouds4Coordination (C4C) federation system [14]. The C4C system is a cross-cloud federation space built using concept of Virtual Enterprise [15] and is utilized for coordination in multi-site construction industry projects. In Architecture/Engineering/Construction (AEC) projects, numerous companies collaborate to produce, store and share numerous BIM models over the life-cycle of the building construction. The C4C system eases the process of coordination by enabling a shared execution space for all participants of AEC projects where they can update, merge and fetch their requisite BIM data objects. The selection of project participants has been a manual procedure with a prevalent risk of inducting a rogue construction discipline jeopardizing the performance of entire AEC project [16].

This paper contributes to the realisation of real-time BIM based project collaboration in construction by assessing the trust and performance of an organisation, to determine its usefulness and reliability for a given construction project. A CoVE approach is proposed for selecting a new collaborating discipline within a construction project. The CoVE index is a threshold value derived in any given context based on i) trust based perceived risk, ii) performance based perceived competence and iii) utility based importance of the new participant. This approach has been verified experimentally, using a real highway bridge construction project provided by Highways England that makes use of the Consensus Assessment Initiative Questionnaire (CAIQ) dataset from CSA Security Trust and Assurance Registry (STAR) [17], and competence evaluated using BIM datasets [18].

The rest of the paper is organized as follows. Section II describes related work, and Section III covers system design for the C4C system. Methodology for calculating the CoVE index is presented in Section IV and experimental evaluation in Section V. Section VI presents the conclusions that can be drawn from this approach.

## II. BASIC CONCEPTS AND RELATED WORK
This section describes the basic concepts of trust evaluation and cloud federation related to multi-disciplinary construction projects collaboration.

### A. TRUST EVALUATION FOR CONSTRUCTION
Trust in an entity has always been used to measure the extent to which the entity will behave as expected. In the context of distributed and multi-agent systems, the concept of trust is mostly bound to the reliability, security and privacy parameters. Trust evaluation mechanisms utilize various indicator values of these parameters collected from sources such as human behavior, perception and interaction experiences with a system. In general, trust sources can be based on i) recommendations, either direct or transitive, provided to a potential user by others based on their own experience, ii) verification of contract signed between the user and the provider to estimate the level of variation from the defined thresholds in policy, and iii) attribute-based assessment by a third party(ies) to verify the capabilities and competencies of collaborative entities.

Trust evaluation in construction based on terms defined in a contract is not suitable for a collaborative framework with heterogeneity in its participants' infrastructures, services, and contracting languages [19]. It is instead necessary to use a commonly agreed set of attributes that can be used as a basis of such an assessment. Since the services / capabilities in construction are leased among the stakeholders, getting feedback for a stakeholder discipline from its counterpart does not seem to be a viable approach. CSA STAR is a certification program based on Cloud Controls Matrix (CCM) framework to support a standardized attribute assessment of cloud providers [17] in the form of CAIQ. The outcome of CAIQ assessment aims to support clients in making informed decisions before adopting/using a discipline when there are no transaction ratings available (i.e. for new market entrants) or there is a likelihood of false ratings or biased feedback (colluding peers/competition).

The earliest work that refers to CAIQ for trust establishment in cloud computing utilizes the concept of trust properties as defined by the CSA self-assessment framework [20]. In a later attempt [21], the authors elaborate their concept by establishing a Trust Management System based on CAIQ. Another framework presented in [22] uses the concept of a trusted Third Party Auditor to support security auditing of a CSP according to security preferences provided by cloud users. However, a detailed working of such a mechanism is not provided by the authors. In [23] authors have proposed a method of utilizing CAIQ assessment and complementing it with user feedback. However, their method of fusion lacks adaptability for dynamic cloud environments. In [24], the authors have proposed to utilize the Cloud Trust Protocol for users to request CAIQ assessment of CSPs in the form of opinions. These opinions are combined with the latest user feedback for the same service.

A joint trust and risk model is introduced in [25] for federated cloud services. The model is based on CAIQ and cloud service providers' performance history extending the work presented in [26]. However, verification of the model is only based on an analytical analysis and does not verify its implications in real life scenarios. The authors in [27] has proposed a cloud service trustworthiness assessment mechanism mainly focusing on security and dependability attributes. The proposed mechanism is based on the capabilities of a CSP

as listed in its CAIQ assessment to evaluate the trustworthiness score of the service. However, the overall assessment is merely an average score of all control domains and hence lacks adaptability in case of a dynamic scenario of cloud federation. Moreover, experimental evaluation of the proposed mechanism is not provided for verifying its usability in cloud scenarios. In [28], a Security Measurement as a Trust framework has been proposed that allows cloud customers to select CSPs based on their security requirement specifications as per CAIQ assessment. The authors recommend Analytical Hierarchical Process model to solve the problem of comparison and multi-criteria decision for cloud customers. However, the details of this model are neither fully elaborated, nor the authors have evaluated the feasibility of their approach by any means.

### B. CLOUD FEDERATION FOR CONSTRUCTION DISCIPLINES

Cloud bridging or federation [3] presents a complex scenario of dynamically sharing resources among different cloud providers. Service composition among heterogeneous participants of the federation may occur at any layer of cloud service delivery model [29]. Various cloud bridging solutions like IBM's Cast Iron Cloud Integration tools [30] are present in the market, and are used in applications development in various environments. Cast Iron integrates with multiple other products and systems from IBM and various other vendors, such as Salesforces and SAP CRM. This helps in integrating locally placed systems with private and public Cloud environments [31] for efficient provisioning and scheduling [32], [33] of cloud resources. Many other bridging solutions such as Oracle Cloud Machine which can connect to an external data center while being deployed on local infrastructure at customer premises are also available. Other similar work includes Munkley *et al.* [34], who have created information synchronization systems between Revit Server and an internal storage server, allowing internal customers to see a read-only copy of the Revit (core) model. Boeykens and Koenraad [35] have developed a layered client/server approach that provides an event based communications pool between components embedded into BIM authoring packages.

Relative to the establishment of trust in cloud based construction projects, the rapid sharing of data also raises the issue of data confidence - acknowledged more commonly in the AEC industry through the use of 'issue status' for physical documents (where documents are provided status equal to what they can be used for reliably and thus what the issuing party assumes responsibility and/or liability for). This is motivated in particular by the governmental objective of achieving full cooperative BIM across the AEC industry (with all project and asset information, paperwork and data being electronic). We address such requirements by developing a ''perceived trust model'' for project collaboration, particularly for determining whether a new participating system can be federated with existing ones.

## III. SYSTEM DESIGN

This section describes the design of a cloud based collaborative system supporting CoVE based discipline selection. Construction projects can involve various organizations ranging from small enterprises to large multinational organizations offering multiple professions and disciplines, each using their in-house or externally sourced computer systems. When these organizations become part of an AEC project, over different time frames, their systems can generate multiple types of data, and be used to carry out processing on such data. Keeping in view this context, a CometCloud based federation space is used to enable collaboration between various disciplines i.e. architects, designers and facility managers etc. for various design and construction tasks. For any project, a discipline joins the C4C system by enabling its cloud infrastructure and data to be a part of a shared federation space. Each discipline can consist of local client (user) machines connected to a cloud system that supports a CometCloud deployment with one master and several worker processes. The C4C system uses a coordination mechanism based on event propagation to the relevant discipline(s). Initially, at the time of project creation, a notification is propagated and a master node (machine) makes a new project on its cloud system in the form of Industry Foundation Classes (IFC) objects. Afterward, the master process receives various tasks related to this project from different disciplines and assign it to workers. These workers execute the tasks and return results to their local master node/process.

From a computational perspective, the project collaboration framework is dynamically created at runtime, where disciplines join or leave based on trust assessment. Each discipline also has multiple processes that carry out actual task executions on locally available resources. A process starts when a client process requests an update (changes one or more IFC object(s)) and terminates when the update is observed at another discipline. This requires an object to be transferred from the client's local machine and to the remote discipline that has requested a view or update. The overheads of the framework are measured with an aggregated time-to-complete (ATTC) metric that depends on the number of IFC objects being executed, the number of simultaneous client requests that need to access the federated model and the number of disciplines that are part of the federation. Section IV-B presents details regarding ATTC with respect to different system operations and the number of disciplines participating in the federation and making updates on IFC objects.

A ''Federation Manager'' (FedMgr) is responsible for managing this entire project collaboration. FedMgr can always retrieve the latest version of the BIM project from the federation space. Responsibilities of FedMgr include (i) requirement identification (ii) operational management and (iii) mediation between all entities involved in an AEC project. The entire C4C system must support various processes, one of which is the addition of a new discipline to the construction collaboration framework as required by the project. Recently, this process of introducing a new discipline
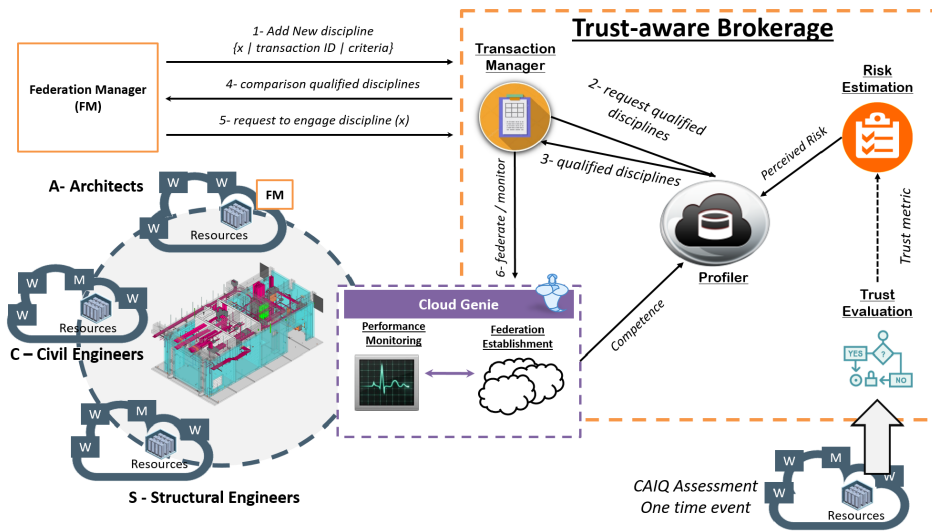
**FIGURE 1.** Trust-aware brokerage architecture and system workflow.

to the BIM project process has not been based on any selection criteria and has risk implications for other (existing) participants.

The extended design of C4C system is illustrated in Figure 1, containing "new" disciplines interacting with existing ones to support the entire project workflow of the proposed system. These additional entities are as follows:

*Cloud Federation Broker:* Trustworthy interactions between different AEC organizations (including FedMgr) within the federation are administrated by a Cloud Federation Broker (CFB). The broker's agent "Cloud Genie" is installed within each successfully registered discipline to keep track of activities and BIM objects when part of the federation. The CFB is responsible for maintaining a *Profile* for every discipline participating in the federation. A discipline's profile maintained with the *FedMgr* is a combined view of its trust based risk assessment (IV-A) and competence (IV-B).

*Certification Source/Cloud Security Alliance:* Audit and assessment based recommendations from CSA are used as a source of trust for a discipline. CSA offers a STAR program with CAIQ framework [17] for cloud security audit, assessment and certification. The certification mechanism ensures that a common approach is used to compare multiple providers. The certification levels proposed by the CSA are also recognized within the community, ensuring that a new provider interested in federation can support pre-defined set of security requirements.

### A. SYSTEM WORKFLOW AND INTERACTIONS

The typical C4C process starts when the construction project manager "FedMgr" engages other disciplines on a project and adds/removes disciplines as needed. Interaction between the FedMgr and CFB is used to support the selection of disciplines from the list of registered (available) disciplines. This request is initiated by FedMgr every time a discipline is to be

added to the project. Each discipline interested in joining the federation has to be registered with the CFB by providing its credentials (name, endpoint, metadata, authentication information etc.) and its CAIQ assessment endorsed by CSA. This CAIQ assessment is an input to the *Trust Evaluation* process, as described in section IV. This process of registration and trust evaluation is a one time process during the membership of any discipline with the CFB.

Once a discipline is registered with the CFB, it can participate in a project by leasing or acquiring resources (or capabilities) as and when required. The CFB maintains a Federated Resource List (FRL) within the *Profiler* repository – keeping information of resources offered by each discipline. This FRL is continuously updated with the help of *cloud genie* which reports resources that are either Waiting to Acquire (WTA) or Ready to Lease (RTL). A WTA is a resource demanded by any discipline that is required by the project and has not yet been matched. An RTL is an additional resource offered by a participant of a federation that has not yet been matched. Any discipline requiring additional capability or resource(s) generates a Request for Resource (RFR) to the FedMgr. The process involved in engaging a discipline is as follows:

1) The *FedMgr* upon receiving a RFR generates a request *add_new_discipline*$\{x, tr_{id}, criteria\}$ and forwards it to the CFB. Here $x$ is a discipline required, $tr_{id}$ is the project identification number and is null for the first time when the federation is yet to be created, *criteria* is any attribute-value pair for the required resource, including trust and competence values.

2) This *RFR* is directed to the Transaction Manager, which verifies the availability of matching resource(s) and respective discipline from the Profiler. Multiple eligible providers for discipline $x$ fulfilling the given *criteria* are then forwarded to the Transaction Manager. The Transaction Manager is responsible for

computing all possible service compositions using eligible disciplines.

3) To support decision making over these service compositions the Transaction Manager may fetch additional details e.g. overall capacity of the requisite disciplines. This allows multiple variables to be taken into account, complementing the trust and performance criteria. This list of service compositions is forwarded to the Federation Manager.

4) The FedMgr generates a Request to Engage (RTE) for that given discipline to engage it in the project. A new transaction is generated whenever an RTE is not associated with any ongoing transaction (i.e. $tr_{id}$ value is null). On the other hand, if the RTE contains a transaction identity, this resource exchange is termed as a sub-transaction of that particular transaction. This entire mechanism starting from the generation of RFR till the engagement of resource(s) by a RTE is a recurring process for any participant of the federation.

5) Adding new discipline to the federation also involves the use of a *cloud genie* to monitor the performance during the project. On project completion, the CFB computes competence of the disciplines involved based on the performance reported by the *cloud genie*.

The complexity of the entire process is determined by the following factors:

- The number of disciplines participating in the collaboration and the amount of data (IFC objects) exchanges
- Number of requests and updates from disciplines requiring access to the federated IFC model
- The number of trust iterations required to evaluate a discipline for participating in a project

As the federation model is based on the coordination of distributed disciplines, this enables information sharing by publishing requests/offers to/for information to this shared data. The complexity is also related to the use of federated management space that orchestrates the different models and disciplines. In the federation, several exchanges of operational messages are taking place for discovering resources, announcing changes at a site, routing disciplines' request to the appropriate site(s), or initiating negotiations to create ad-hoc federation execution spaces. To enable the federation to coordinate access to resources for the execution of a particular set of tasks, a master discipline needs to manage tasks execution or delegate this role to a dedicated discipline when some specific objects or model functionality is required.

## IV. COOPERATION VALUE ESTIMATION

The proposed CoVE evaluates the benefit of discipline $x$ for a Project '$\alpha$', given a context of use $c$ and is represented by:

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

where *Perceived Risk*$(x, \alpha, c)$ is inversely related to the trust value of a discipline. *Perceived competence*$(x, c)$ of a discipline $x$ is based on its performance as monitored by *FedMgr*, whereas $T(x, c)$ is a cumulative effect of historical performance evaluations, if any. In equation 1, $I(x, \alpha, c)$ is the importance of collaborating with a discipline (for context $c$) as anticipated by the owner of the project $\alpha$. The equation 1 is also valid for any generalized context of collaboration.

### A. PERCEIVED RISK

Every discipline must maintain its profile with the CFB during membership in the C4C system. This profile serves to give a collective view of risk assessment and competence of a project discipline. In case a discipline joins the federation for the first time and it has no performance history registered with the CFB, its profile is only based on its trust posture:

$$perceived\ risk \propto \frac{1}{trust\ posture} \quad (2)$$

"trust posture" measures the disciplines' ability to conform to CSA recommendations. However, it should never be out of context for which the discipline is being engaged [36]. For example, a particular discipline may be required as a storage repository in the federation. Context awareness requires that instead of all provided CAIQ controls, trust for this discipline should be evaluated only over those controls that are relevant to storage. The proposed research however takes into account a generic context of trust evaluation based on all CAIQ controls. For any discipline, control domains in its CAIQ assessment are modeled as respective opinions for that discipline using subjective belief theory [37]. Each opinion is an aggregated view of positive and negative declarations that a discipline has made for assertions of CAIQ. Considering a generalized case of collaboration i.e. when no particular context is provided, given $p$ as positive, $q$ as negative, *un* as unanswered and *NA* as not applicable declarations with $N = (p + q + un)$ as the total assertions applicable, the trust of a discipline can be given as:

$$T(\lambda, \gamma, \varphi, \epsilon) = \lambda + \varphi * \epsilon \quad (3)$$

given

$$\lambda = \rho * \zeta; \quad \gamma = \eta * \zeta; \quad \varphi = 1 - \zeta; \quad (4)$$

$$\rho = \frac{p}{p + q}; \eta = \frac{q}{p + q};$$

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

In equation 4, parameters $\lambda$, $\gamma$ and $\varphi$ is the belief, disbelief and uncertainty of the behavior associated with a discipline respectively. $\rho$ and $\eta$ are the average positiveness and negativeness of a domain respectively based on $p$ and $q$ for each domain. Confidence $\zeta$, is evaluated on the basis of $p$ and $q$, with $N = (p + q + un)$ and an optimistic initial expectation of $\epsilon = 0.99$. The global trust value $T$ of a discipline is the aggregated opinion for all domains respective to the context $c$.

**TABLE 1.** Individual trust representation of five disciplines.

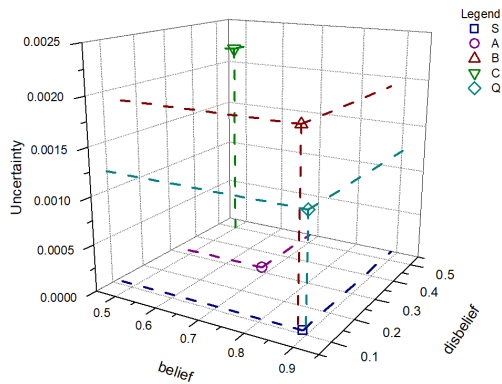| CSP | N | p | q | un | $\lambda$ | $\gamma$ | $\varphi$ | T |
|-----|-----|-----|-----|-----|--------|--------|--------|--------|
| S | 272 | 228 | 44 | 0 | 0.8382 | 0.1618 | 0 | 0.8864 |
| A | 290 | 208 | 82 | 0 | 0.7172 | 0.2828 | 0 | 0.7172 |
| B | 295 | 211 | 31 | 53 | 0.8706 | 0.1279 | 0.0015 | 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 |



**FIGURE 2.** Representation of individual trust values of project discipline.

Using equations 3-5, Table 1 provides values for $N, p, q$ and *un* evaluated from the CAIQ data of five random disciplines, for example, S, A, B, C, and Q, present in CSA STAR database [17]. The values of $p$ and $q$ represent the total number of positive and negative declarations, whereas values of *un* represent assertions left unanswered by the discipline. These three values are afterward aggregated as the total number of applicable assertions $N$. The trust parameters i.e. belief, disbelief and uncertainty are represented in Figure 2 for all disciplines along X-axis, Y-axis and Z-axis respectively. Among all these given disciplines, Q is rated the best for having the maximum trust value.

## B. PERCEIVED COMPETENCE

Perceived competence is the measurement of overall performance of a given discipline provider for tasks assigned to it during any given time frame. Since C4C is a batch processing system, two levels of competence can be evaluated i.e. the entire project completion time as project competence, and task based competence for individual disciplines. Project performance is used to measure the success or failure of identifying a group of disciplines through different selection criteria. Task based competence of each discipline is based on the number of IFC objects assigned to it and the time taken by the discipline to process them.

Referring to Figure 3, a local client at discipline A has created the C4C project and now requires to update it in the shared federation space so that other disciplines may work on it as per their role in the project. For example, considering discipline A as Architects, who have finalized an outline of a building as required by the customer, it should now be updated to the civil engineering discipline C or any other. The update process starts when the local client A pushes the model

data into its cloud. The cloud owned by discipline A writes the new objects and their metadata on the disk. Afterward a metadata hashmap is created and advertised in the shared federation space. All sites receive the update notification and update the metadata for the C4C project. This process of update is represented in Figure 3 by Update Start and Update Finish. The amount of time taken from U1 to U6 is called 'update time' and is given by *update_time* = *write_time* + *sync_time*. Similar process of update is followed every time whenever a discipline 'N' updates a model with any newer version *v* in the shared space. This results in a similar round of notifications and metadata propagated to interested site(s). All sites eligible for new version *v* updates their metadata with this version so that they may fetch it at any later stage if required.

During the lifetime of a project, a participating discipline may want to *fetch* a recent version of the BIM model to work on it. Figure 3 shows a Civil Engineering discipline C interested to work on the model updated by discipline A. The fetch process from discipline C is represented to occur between 'Fetch Start' and 'Fetch End' in Figure 3. This includes finding a location for all the BIM objects marked as updated in the metadata, requesting the discipline(s) for updated model(s), receiving model(s), merging all the different updates and writing the model in the shared space. Once a merged model is created for a given discipline, it is returned to the local client for that discipline for requisite working and updates. The total time it takes for the fetch process starting from F1-F8 in Figure 3 is denoted by the fetch time. Update and fetch times are utilized as individual perceived competence of any given discipline as given in equation 6.

$$perceived\ competence = \frac{number\ of\ IFC\ objects\ processed}{time\ taken} \quad (6)$$

The ATTC metric for a project is a sum of all these individual times: (i) object writing time $T_w$, (ii) metadata synchronization time $T_s$ and (iii) fetch overhead time $T_f$, for the entire project i.e. $ATTC = T_w + T_s + T_f$. The ATTC measurement is applied to the entire project and is counted towards the success of collaboration in terms of performance. The global project performance is then given by equation 7.

$$project\ performance = \frac{num\ objects\ processed\ in\ project}{ATTC} \quad (7)$$

## V. EXPERIMENTAL EVALUATION

This section describes the implementation details and the methodology used for experimentation and evaluation of the proposed approach. Data acquisition and system settings are also described in this section to elaborate further experimentation and extensions to basic work.

## A. IMPLEMENTATION

The implementation of a trust-aware model for cross-cloud federation has been carried using a custom built Trusted Third
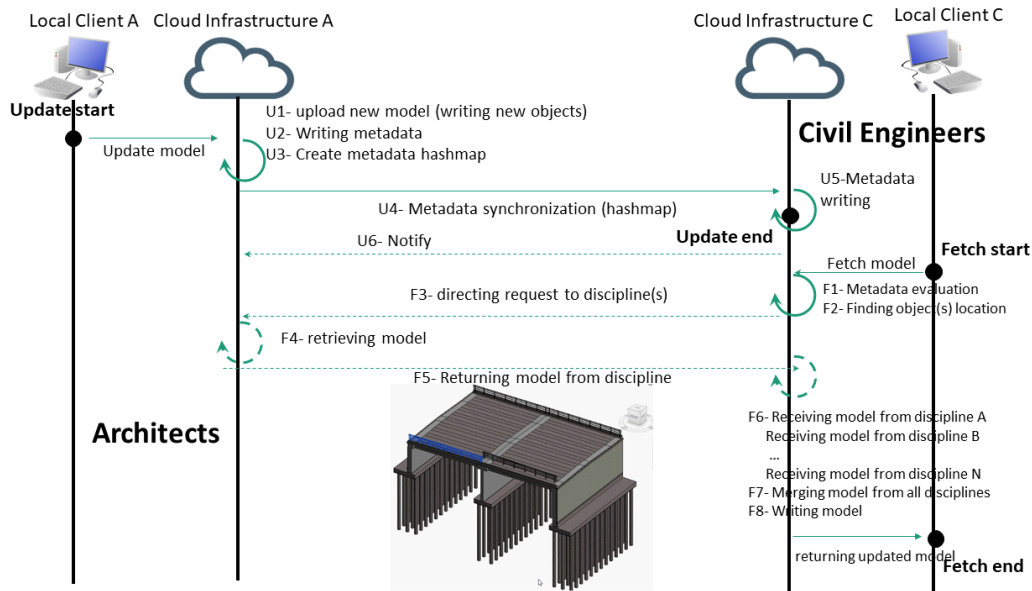
**FIGURE 3.** Perceived competence metric and project disciplines workflow.

**TABLE 2.** Quantitative parameters of proposed research.

| Metric | Parameter | Description |
|---|---|---|
| Trust | Positiveness | Average number of positive declarations for any CSP |
| | Negativeness | Average number of negative declarations for any CSP |
| | Belief | The expected behaviour based on positiveness |
| | Disbelief | The expected behaviour based on negativeness |
| | Uncertainty | Uncertainty in expectation |
| | Initial expectation | Prior knowledge regarding expectations |
| | Individual Trust | Expected trust value based on belief, disbelief and uncertainty of a CSP |
| | Perceived Risk | Risk of engaging a CSP in the formation of a composite service |
| Time | Writing time | Time taken by a CSP to write workload data (objects) |
| | Synchronization time | Time taken by all CSPs to synchronize metadata for data objects put within the shared execution space |
| | Update time | Total time taken by a workload to be written to shared federation space and metadata to get synchronized in federation |
| | Fetch time | Time taken by a CSP to fetch workload updates from shared execution space |
| | Aggregated time-to-complete | Time taken by the project to complete. A project may involve multiple object updates and fetches by any service provider |
| Decision | Write Performance | Number of Objects written to disk per seconds by a CSP |
| | Synchronization performance | Number of metadata objects synchronized per seconds by a CSP |
| | Update performance | Number of objects updated per seconds |
| | Perceived Competence | Number of objects per ATTC |
| | Project Performance | Performance of the entire project with any chosen set of CSPs |
| | CoVE | Expected value to decide whether to engage in resource exchange with a CSP |

Party broker and its agent built using CPython. They are integrated with the C4C federated cloud system built using Cometcloud [13] federation framework. The broker agent resides within the cloud providers infrastructure and makes use of Linux system level commands to obtain trust and performance data from C4C nodes. This trust and performance data is expressed in the form of quantitative parameters described in Table 2. The proposed CoVE approach is implemented as a part of CFB written in CPython and executed as a service. SQLite serves as a repository to store all data related to this system including discipline details, trust evaluation and transaction details, etc. The virtualized environment consists of 10 nodes (one trust-aware CFB node and nine disciplines) that have been deployed in Google Cloud Platform datacenter, across multiple availability zones. All compute nodes are running with the specifications given in Table 3. The nine disciplines represent 3 different categories of C4C disciplines

**TABLE 3.** System specification for experimentation.

| Type | OS | Compute | Memory | Storage | Region |
|---|---|---|---|---|---|
| C4C Nodes | Ubuntu 16.04.5 LTS | 1 vCPU | 3.75 GB | 10 GB | europe-west2-a (3), us-east1-b (3), asia-east1-a (2), europe-west4-a (1) |
| Trust-aware broker | — same as above — | | | | asia-south1-a (1) |

with each category having three competitors. All nodes have different trust and performance levels.

At the functional level, the overheads of the framework are related to a set of individual operations such as object writing time, metadata synchronization time and overhead associated with the retrieval of the entire project. Overheads are identified with a metadata model that is used to store information about each object and a versioning system records all the versions that an IFC object may have over time. At the

framework level, overheads are also identified for the data exchange stage where data tuples are utilized to comply with requirements related to data processing, data sharing and data storage. In addition to these, there are also overheads associated with the event propagation mechanism for monitoring the various operations appearing when working with IFC objects. Overheads are related to the complexity of the data workflow, as the successful delivery of a construction project is a highly complex process; requiring collaboration between multiple disciplines where an increased quantity of data needs to be exchanged. Disciplines such as designers, suppliers and facilities managers have specific requirements therefore the federation and associated trust evaluation need to address a range of design and construction tasks with increased complexity. Considering the particular case of trust evaluation, the overheads of the process are significantly low as compared to the underlying federation processes. Moreover, trust evaluation being a centralized process is linearly dependent on the number of federation participants and scale well in case the number of disciplines is increased.

### B. DATA COLLECTION

Experimental evaluation of the proposed model makes use of two types of quantitative datasets i.e. CAIQ based cloud audit reports and BIM models. A set of CAIQ assessments of various reputable CSPs having level-2 STAR certification has been obtained from CSA STAR registry [17]. The recent literature on trust evaluation identifies several other authors who have also made use of this data set [20]–[27].

The proposed research has used the data published in CAIQ v3.0.1 format from CSPs that include, but are not limited to Acer Cyber Center Services, Amazon, GitHub, Google, IBM, SAP and Salesforce etc. The CSA STAR registry enables a standards-based, community wide perspective on cloud security offerings, enabling end users to "accelerate their due diligence and leading to higher quality procurement experiences". The registry uses several industry standards, such as CCM, CAIQ (as used in this work), and the Cloud Audit and Control Trust Protocol. The CSA has worked with many international certification agencies, e.g. European Security Agency (ENISA) and the Chinese CEPREI, ensuring that the outcome has a wider applicability across several different international markets. The associated CSA STAR Watch initiative provides a tool in a database structure to monitor and assess public and private cloud providers.

The performance results are acquired by using real trial data and processes provided by project partner Costain Group PLC. The benchmarks are based on observations retrieved from one of their real projects identifying the Highways England construction of a new bridge on the A556. This project involves different disciplines contributing various amounts of data related to different parts of the structure (see Figure 3). Every project $P$ (groups of tasks $P = T_1, T_2, T_3, \ldots . T_n$ where $T = update|fetch$) is considered to be completed when each discipline has at least *i) made one update to the project* and *ii) fetched one version of the final model from*
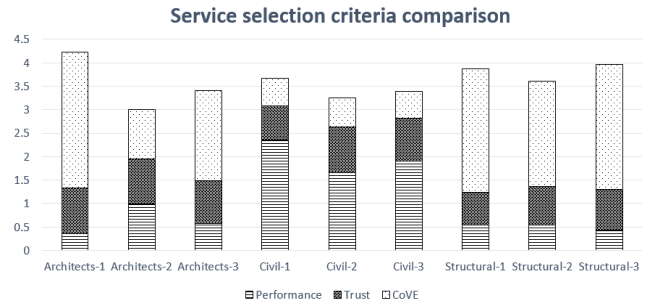


**FIGURE 4.** CoVE based service selection for the construction project.

*the shared space*. For every task, the total time of completion is considered as defined in [14] with the exception that time epoch starts when the data arrives at the discipline instead of starting when the user sent it. This epoch ends when the FedMgr receives the notification of completion from the subscribers for the assigned tasks. Moreover, the individual performance of each subscriber (discipline) is also measured at the fine-grained level for every task. This time epoch starts when the task is received at the discipline and ends when the task is finished and reported back to the publisher. For each site the risk is measured as the interval $\Delta t$ equal to the time over which a discipline remains offline due to its security vulnerabilities, and is considered inversely proportional to its CAIQ based trust. It is assumed that the higher the trust, the lower will be the time that a discipline remains offline and hence lesser risk to the project.

The experimentation aims to evaluate the i) performance efficiency and ii) accuracy of the proposed approach. The efficiency of the system is measured in terms of its performance in different scenarios of varying workloads i.e. model sizes of i) 300KBs mentioned as default model ii) 689KBs iii) 956KBs iv) 3.44MBs v) 5.34MBs and vi) 8.94 MBs. The accuracy of a system depends on the fact that the system is successfully able to identify reliable and trustworthy service compositions. Moreover, these experiments aim to observe how the perceived risk is related to delays in the project.

### C. EXPERIMENT-1

This experiment explains the basic working of the proposed approach. In this experiment the usage of CoVE index in the selection of a discipline provider is described. A total of three disciplines i.e. Architecture, Civil Engineering and Structural Engineering are required to execute a construction project. For each discipline, three different providers (a total of 9 discipline providers) are offering their respective expertise with performance, trust and cooperation index values. A discipline provider is said to be the best possible selection if it has the lowest CoVE index. Among all the available disciplines, the Architects-2, Civil-3 and Structural-2 are the best CoVE based selection in their respective domains as shown in Figure 4. Moreover, in case the selection is based on performance, Architect-2, Civil-1 and Structural-1 are the possible choices. Also, in the case of higher
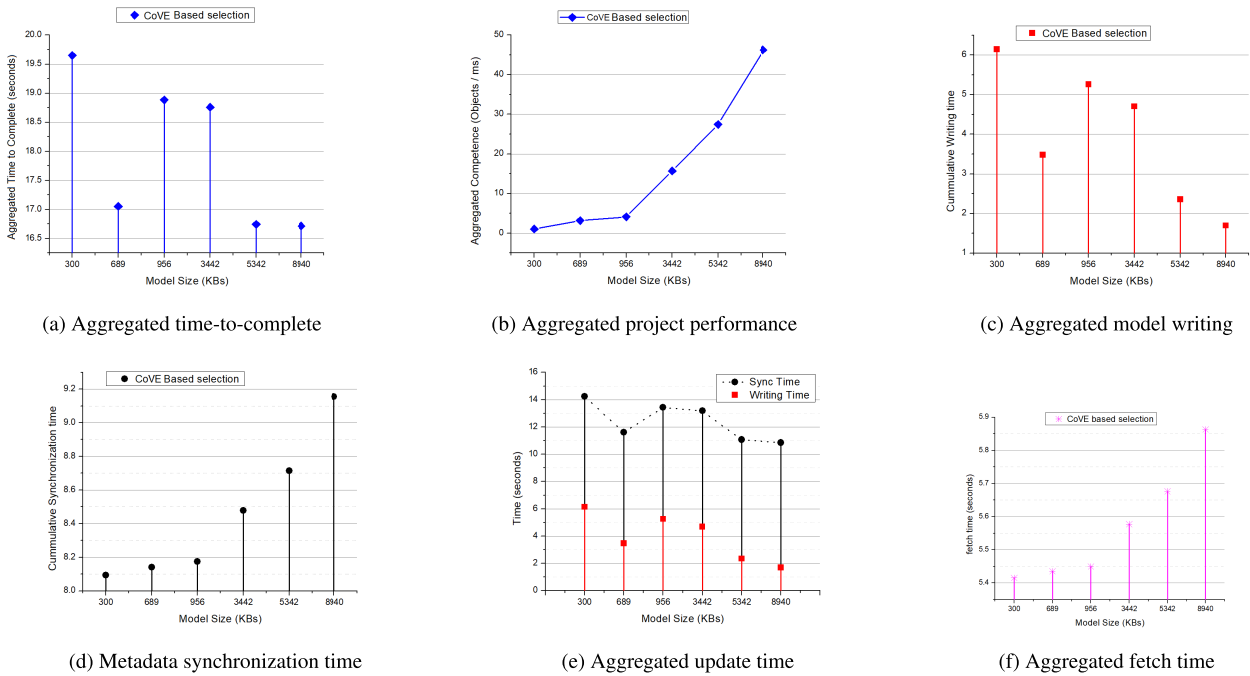
(a) Aggregated time-to-complete

(b) Aggregated project performance

(c) Aggregated model writing

(d) Metadata synchronization time

(e) Aggregated update time

(f) Aggregated fetch time

**FIGURE 5.** Various metrics measured for experiment 2.

trust, the Architects-1, Civil-2 and Structural-3 are the best choices.

### D. EXPERIMENT-2

In this experiment, the discipline providers are selected based on the proposed CoVE indexes. These disciplines are then engaged to execute the different types of workloads as described in the previous section. For each discipline, out of all candidate discipline providers, the one with the best CoVE index is selected i.e. Architects-2, Civil-3 and Structural-2 to measure the overall project completion time as shown in Figure 5 (a).

This ATTC is the cumulative time of parsing and writing the model in the federation space given in Figure 5 (c) along with the synchronization of metadata in Figure 5(d) and fetching time as shown in Figure 5 (e) for all disciplines. The ATTC given in Figure 5 (a) depicts that time taken for smaller sized model is greater than the time taken for large sized model. The project performance in terms of aggregated competence of all disciplines is shown in Figure 5 (b). This figure shows the lesser performance of project in case of smaller models and higher performance as the model size is increased. Figure 5 (c) depicts the cumulative model writing time for the project with the maximum time taken by the smallest model and the lowest writing time for the largest model size. Figure 5 (d) shows the metadata synchronization time for all workloads and depicts a linear increase in the synchronization times. The writing time and synchronization time are collectively shown as update time in Figure 5 (e). It shows aggregated update times for the given workloads. The overall fetch time for the workloads as illustrated in
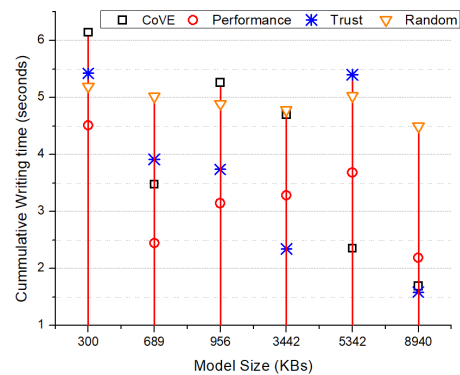


**FIGURE 6.** Model writing time measured for all selection criteria.

Figure 5 (f) also follow a linear approach scaling from lower to higher times concerning increase in the size of the model.

### E. EXPERIMENT-3

In this experiment, the validity of the proposed CoVE approach has been verified by comparing it with three different service selection criteria based on benchmarks for i) performance [38] ii) trust [20], [21] and iii) random combination of trust, performance and CoVE index. In all of the three cases, the selected disciplines are engaged to execute a variety of similar workloads as described at the start of this section. The experiments are performed to measure various performance parameters (Table 2) including i) writing time as in Figure 6, ii) synchronization time as in Figure 7 and iii) fetch time as in Figure 8, iv) cumulative project performance
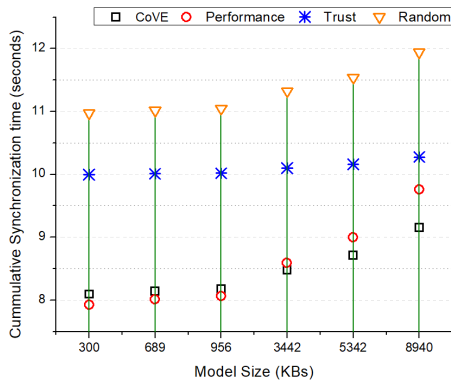
**FIGURE 7.** Comparison of model synchronization time measured for all selection criteria.
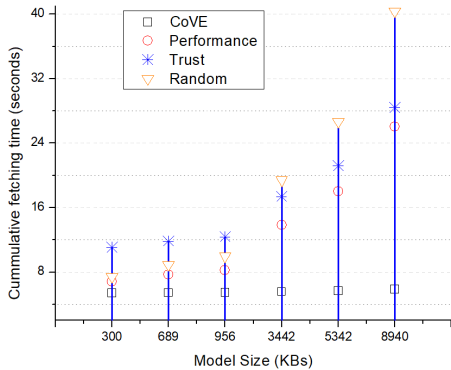


**FIGURE 8.** Model fetching time for all selection criteria.



**FIGURE 9.** Comparison of project performance in case of various selection criteria.



**FIGURE 10.** Comparison of aggregated time-to-complete for various projects.

as an aggregated competence of all disciplines shown in Figure 9 and v) ATTC of a project as in Figure 10.

Figure 6 refers to model writing time for all selection criteria. This figure shows lots of variation in writing times for all selection criteria as the model size is increased. This variation in writing time is due to the number of objects received and the level of details for each object processed and written by the C4C worker. In the case of synchronization times in Figure 7, less time is taken by performance based selection for small model size. However, the proposed approach surpasses all other selection criteria with lesser synchronization times as the model size is increased. The comparison for overall fetch time for all selection criteria is illustrated in Figure 8. All criteria show a linear increase in fetch time scaling from lower to higher times concerning increase in the size of the model. The proposed CoVE approach has been consistent in spending a lot less time in model fetching than all other criteria.

The above mentioned direct variables are afterward used to compare the efficiency of the proposed approach with all selection criteria. A consolidated view of project performance and ATTC has been depicted in Figure 9 and Figure 10 respectively. From Figure 9 it can be observed that for larger models the CoVE approach has been efficient in maintaining a higher efficiency than performance based selection. Since the CoVE index is not solely dependent on perceived risk, manipulating the performance can enable a discipline to com-
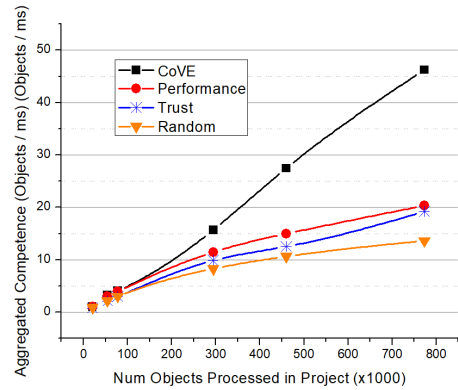
pete with a lower threshold but it is unable to cope with large workloads. Such a discipline gains its CoVE index by performing shorter duration tasks and have taken benefit of its ability to complete those tasks before going offline due to its vulnerabilities. However, they are not able to maintain CoVE index in the case of large models, thus introducing higher risk for the entire project. Moreover, as evident from Figure 10, the ATTC for CoVE based selection has always remained consistent with the increase in workload size. A slight variation can be observed in ATTC only due to the writing time. This variation is a result of the setup time that each discipline takes to start processing a model. Smaller models have to wait for the same amount of time as compared to large models, however, the number of objects processed in smaller models is fewer than large models and eventually contribute to their lack of performance.

## VI. CONCLUSION
Large construction projects require multiple organizations to participate and share data and computational infrastructure. Such collaborations are required to be based on trust and competence for establishing and sustaining long term relationships. This research has demonstrated how such trust evaluation can be utilized as a method of selecting a partner able to deliver infrastructure capability to meet the requirements of other participants in the consortium. The compu-

tational infrastructure considered in this work is primarily used to store data (e.g. BIM data objects) and undertake analysis on such data. We refer to this infrastructure capability as the "competence" of the partner/discipline. Another aspect used to support partner selection is the audit and assessment process associated with the security credentials of the participant, and based on a methodology used by CSA. We suggest that in a multi-participant project involving federation of computational infrastructure across different partners, security credentials play an essential role. The CSA methodology involves using a questionnaire to certify (either as a self-certification or through a pre-agreed third party) an infrastructure provider. Using this approach, a *discipline* (e.g. architects, engineers) can make use of computational infrastructure that is self-operated/managed, or leased from an external cloud provider. In both instances, the combined use of security credentials and capability (i.e. offered services) can be used to support selection. As our experiments demonstrate, in a marketplace consisting of different instances of a given discipline (e.g. three companies providing facilities management expertise), these two factors (security & competence) can be used to undertake selection. This approach helps to quantify whether a construction organization could be a part of the cloud collaboration framework or not. Various experiments have shown that other mechanisms for discipline selection may surpass the proposed method for shorter duration projects. However, a selection using the proposed approach helps identify partners offering capability that can maintain project performance over a long time frame for construction projects.

## REFERENCES

[1] H. Yuan, J. Bi, W. Tan, M. Zhou, B. H. Li, and J. Li, "TTSA: An effective scheduling approach for delay bounded tasks in hybrid clouds," *IEEE Trans. Cybern.*, vol. 47, no. 11, pp. 3658–3668, Nov. 2017.

[2] H. Yuan, J. Bi, W. Tan, and B. H. Li, "Temporal task scheduling with constrained service delay for profit maximization in hybrid clouds," *IEEE Trans. Autom. Sci. Eng.*, vol. 14, no. 1, pp. 337–348, Jan. 2017.

[3] A. N. Toosi, R. N. Calheiros, and R. Buyya, "Interconnected cloud computing environments: Challenges, taxonomy, and survey," *ACM Comput. Surveys*, vol. 47, no. 1, pp. 1–47, Jul. 2014.

[4] C. Huxham and S. Vangen, "Working together. Key themes in the management of relationships between public and non-profit organizations," *Int. J. Public Sector Manage.*, vol. 9, no. 7, pp. 5–17, Dec. 1996.

[5] B. Gray and D. J. Wood, "Collaborative alliances: Moving from practice to theory," *J. Appl. Behav. Sci.*, vol. 27, no. 1, pp. 3–22, Mar. 1991.

[6] J. Child and D. Faulkne, *Strategies of Cooperation: Managing Alliances, Networks, and the United Kingdom*. Berlin, Germany: Physica-Verlag, 1998.

[7] F. McDonald and J. Genefke, *Effective Collaboration: Managing the Obstacles to Success*. London, U.K.: Palgrave, 2001.

[8] R. J. Bies, T. Tripp, R. Kramer, and T. Tyler, *Trust in Organizations: Frontiers of Theory and Research*. Thousand Oaks, CA, USA: Sage, 1996, pp. 246–260.

[9] C. Lane and R. Bachmann, "The social constitution of trust: Supplier relations in Britain and Germany," *Org. Stud.*, vol. 17, no. 3, pp. 365–395, May 1996.

[10] S. Vangen and C. Huxham, "Nurturing collaborative relations: Building trust in interorganizational collaboration," *J. Appl. Behav. Sci.*, vol. 39, no. 1, pp. 5–31, 2003.

[11] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not so different after all: A cross-discipline view of trust," *Acad. Manage. Rev.*, vol. 23, no. 3, pp. 393–404, Jul. 1998.

[12] S. P. Marsh, "Trust in distributed artificial intelligence," presented at the 4th Eur. Workshop Modelling Auton. Agents Multi-Agent World, Berlin, Germany, 1994.

[13] H. Kim and M. Parashar, *CometCloud: An Autonomic Cloud Engine, in Cloud Computing: Principles and Paradigms*. Hoboken, NJ, USA: Wiley, 2011, pp. 275–297. [Online]. Available: http://dx.doi.org/10.1002/9780470940105.ch10

[14] T. H. Beach, O. F. Rana, Y. Rezgui, and M. Parashar, "Cloud computing for the architecture, engineering & construction sector: Requirements, prototype & experience," *J. Cloud Comput., Adv., Syst. Appl.*, vol. 2, no. 1, p. 8, 2013.

[15] I. Petri, T. Beach, O. F. Rana, and Y. Rezgui, "Coordinating multi-site construction projects using federated clouds," *Autom. Construct.*, vol. 83, pp. 273–284, Nov. 2017.

[16] I. Petri, T. Beach, Y. Rezgui, I. E. Wilson, and H. Li, "Engaging construction stakeholders with sustainability through a knowledge harvesting platform," *Comput. Ind.*, vol. 65, no. 3, pp. 449–469, Apr. 2014.

[17] cloudsa. (2018). *SA Security, Trust & Assurance Registry (STAR)—Cloud Security Alliance*. Accessed: Sep. 12, 2018. [Online]. Available: https://cloudsecurityalliance.org/star/overview

[18] A. Redmond, A. Hore, M. Alshawi, and R. West, "Exploring how information exchanges can be enhanced through cloud BIM," *Autom. Construct.*, vol. 24, pp. 175–183, Jul. 2012.

[19] U. Ahmed, I. Raza, and S. A. Hussain, "Trust evaluation in cross-cloud federation: Survey and requirement analysis," *ACM Comput. Surv.*, vol. 52, no. 1, p. 19, 2019.

[20] S. M. Habib, V. Varadharajan, and M. Muhlhauser, "A trust-aware framework for evaluating security controls of service providers in cloud marketplaces," in *Proc. 12th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jul. 2013, pp. 459–468.

[21] S. M. Habib, S. Ries, M. Mühlhäuser, and P. Varikkattu, "Towards a trust management system for cloud computing marketplaces: Using CAIQ as a trust information source," *Secur. Commun. Netw.*, vol. 7, no. 11, pp. 2185–2200, Nov. 2014.

[22] S. S. Rizvi, T. A. Bolish, and J. R. Pfeffer, "Security evaluation of cloud service providers using third party auditors," in *Proc. 2nd Int. Conf. Internet Things, Data Cloud Comput. (ICC)*, 2017, pp. 1–6.

[23] S. Rizvi, J. Ryoo, J. Kissell, W. Aiken, and Y. Liu, "A security evaluation framework for cloud security auditing," *J. Supercomput.*, vol. 74, no. 11, pp. 5774–5796, Nov. 2018.

[24] A. Algamdi, F. Coenen, and A. Lisitsa, "A trust evaluation method based on the distributed Cloud Trust Protocol (CTP) and opinion sharing," presented at the Int. Conf. Comput. Appl. Technol., (ICCAT), 2017.

[25] E. Cayirci and A. S. de Oliveira, "Modelling trust and risk for cloud services," *J. Cloud Comput.*, vol. 7, no. 1, p. 14, Dec. 2018.

[26] E. Cayirci, A. Garaga, A. Santana de Oliveira, and Y. Roudier, "A risk assessment model for selecting cloud service providers," *J. Cloud Comput.*, vol. 5, no. 1, p. 14, Dec. 2016.

[27] J. Kanpariyasoontorn and T. Senivongse, "Cloud service trustworthiness assessment based on cloud controls matrix," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2017, pp. 291–297.

[28] O. Ghazali, A. M. Tom, H. M. Tahir, S. Hassan, S. A. Nor, and A. H. Mohd, "Security measurement as a trust in cloud computing service selection and monitoring," *J. Adv. Inf. Technol.*, vol. 8, no. 2, pp. 100–106, 2017.

[29] R. B. Bohn, C. A. Lee, and M. Michel, "The NIST cloud federation reference architecture," NIST, Gaithersburg, MD, USA, Tech. Rep. 500-332, Feb. 2020.

[30] Solution. *IBM CastIron*. Accessed: May 21, 2018. [Online]. Available: https://www-01.ibm.com/software/integration/cast-iron-cloud-integration/salesforce-integration/

[31] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST, Gaithersburg, MD, USA, Tech. Rep. 800-145, Sep. 2011.

[32] H. Yuan, J. Bi, and M. Zhou, "Multiqueue scheduling of heterogeneous tasks with bounded response time in hybrid green IaaS clouds," *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5404–5412, Oct. 2019.

[33] H. Yuan, J. Bi, and M. Zhou, "Spatiotemporal task scheduling for heterogeneous delay-tolerant applications in distributed green data centers," *IEEE Trans. Autom. Sci. Eng.*, vol. 16, no. 4, pp. 1686–1697, Oct. 2019.

[34] J. Munkley, M. Kassem, and N. Dawood, "Synchronous building information model-based collaboration in the cloud: A proposed low cost IT platform and a case study," in *Proc. Comput. Civil Building Eng.*, Jun. 2014, pp. 89–96.

[35] S. Boeykens and N. Y. S. Koenraad, "Interactive bi-directional BIM model and application linking," in *Proc. IASS Annu. Symp.*, Aug. 2015, pp. 1–11.

[36] U. Ahmed, I. Petri, O. Rana, I. Raza, and S. A. Hussain, "Risk-based service selection in federated clouds," in *Proc. IEEE/ACM Int. Conf. Utility Cloud Comput. Companion (UCC Companion)*, Dec. 2018, pp. 77–82.

[37] A. Jøsang, "The right type of trust for distributed systems," in *Proc. Workshop New Secur. Paradigms (NSPW)*, 1996, pp. 119–131.

[38] I. Petri, O. F. Rana, T. Beach, and Y. Rezgui, "Performance analysis of multi-institutional data sharing in the Clouds4Coordination system," *Comput. Electr. Eng.*, vol. 58, pp. 227–240, Feb. 2017.

**USAMA AHMED** received the M.S. degree in information security from the National University of Science and Technology (NUST), Islamabad, and the Ph.D. degree in computer science from COMSATS University Islamabad, Lahore Campus specializing in trust-aware cloud systems. He had served as a Project Manager for network security planning and architecture along with security policy formulation and risk assessment with information security management system (ISMS), Pakistan Airforce (PAF). Since 2012, he has been working as a Lecturer with Government College University, Faisalabad. He has numerous publications on his account in conferences and impact factor journals. His research interests include network and cloud security, risk management, and trust-aware distributed systems.

**IOAN PETRI** (Member, IEEE) received the Ph.D. degree in computer science and specializes in intelligent systems, building information modeling, cloud and edge computing, and data analytics. He is currently a Lecturer in smart infrastructure informatics. He is also an Inventor and the ICT Leader of the CUSP platform He has published over 60 peer-reviewed articles in high impact journals and conferences in the field of applied distributed systems and energy management. His research interests include developing intelligent computer systems to create persistent forms of intelligence and user-centric ecosystems in smart buildings and infrastructures. He has served on the program committees of more than 20 international conferences and workshops.

**OMER RANA** (Member, IEEE) received the B.Eng. degree in information systems engineering from the Imperial College (London University), the M.Sc. degree in microelectronics from the University of Southampton, and the Ph.D. degree in neural computing and parallel architectures from the Imperial College (London University). He worked as a Software Developer with London-based Marshall Bio-Technology Ltd., prior to joining Cardiff University, where he developed specialist software to support biotech instrumentation. He is currently a Professor of performance engineering with Cardiff University. He is also a Fellow of the Data Innovation Research Institute, Cardiff University's multidisciplinary. He has contributed to specification and standardization activities via the Open Grid Forum. He contributed to public understanding of science, via the Wellcome Trust funded Science Line, in collaboration with BBC and Channel 4. His research interests are in high-performance distributed computing, data analysis/mining, and multiagent systems. He is a Founding Member and an Associate Editor of *ACM Transactions on Autonomous & Adaptive Systems*. He serves on the Editorial Boards as an Associate Editor for the IEEE Transactions on Parallel and Distributed Systems, (formerly) the IEEE Transactions on Cloud Computing, the *IEEE Cloud Computing Magazine*, and *ACM Transactions on Internet Technology*.

**IMRAN RAZA** (Member, IEEE) received the B.S. and M.Phil. degrees in computer science from Pakistan. Since 2003, he has been working as an Assistant Professor with the Department of Computer Science, COMSATS University Islamabad, Lahore Campus. He has been actively involved in simulating CERN O2/FLP upgrades. He has supervised and co-supervised many funded projects related to ICT in healthcare. He has authored and coauthored more than 40 journal articles and conference papers. His areas of research interests include cloud computing, mobile edge computing, SDN, NFV, wireless sensor networks, MANETS, QoS issue in networks, and routing protocols. He has been a member of ACM.

**SYED ASAD HUSSAIN** (Member, IEEE) received the master's degree from Punjab University Lahore, Pakistan, then he proceeded to the U.K. for his master's from the University of Wales, Cardiff, U.K., and the Ph.D. from the Queen's University Belfast, U.K. Since 2005, he has been leading Communications Networks Research Group, Department of Computer Science, COMSATS University Islamabad, Lahore campus. He was the Head of the Computer Science Department, COMSATS University Islamabad, from 2008 to 2010 and from 2011 to 2017. Since 2010, he has been working as a Professor and the Dean of the Faculty of Information Sciences and Technology, COMSATS University Islamabad, Pakistan, since 2015. He is currently supervising Ph.D. Students at COMSATS University and split-site Ph.D. students at Lancaster University, U.K., in the areas of cloud computing and cybersecurity. He is actively involved in collaborative research with CERN in Switzerland and different universities of the world, such as Cardiff University, U.K., Lancaster University, U.K., Dalhousie University, Canada, and Charles Sturt University, Australia. He is supervising funded projects as a Principal Investigator in the field of healthcare systems. He was funded for his Ph.D. by Nortel Networks, U.K. He has taught at Queen's University Belfast, U.K., Lahore University of Management Sciences (LUMS), and the University of the Punjab, Pakistan. He has authored and coauthored more than 85 journal articles and conference papers. He has written a book titled *Active and Programmable Networks for Adaptive Architectures and Services* (Taylor and Francis USA). He was awarded prestigious Endeavour Research Fellowship by Australian Government for his master's with The University of Sydney, Australia, in 2010. He regularly reviews international journals articles and conferences papers.

● ● ●