Edge-Cloud Resource Federation for Sustainable Cities

Abstract

As cloud computing becomes the dominant mechanism for delivery of electronic services, significant recent effort has focused on certifying cloud services to ensure their compliance with security and privacy standards (such as GDPR). Assessing the benefit of using a particular cloud service, especially if such a service is being offered by providers that may be new to the cloud marketplace, remains a challenge. Cloud Security Alliance (CSA) provides a certification approach that associates a ranking to providers based on their capability assessment using a “cloud control matrix”. A provider can make a self-assessment, or an assessment can be undertaken by a third party. The intention is to increase user *trust* in a provider based on their rating using this methodology. This work investigates whether a similar certification methodology can be applied to edge resources, especially if these edge resources are combined with cloud services in a ”smart cities” context. Can a CSA-like approach also be used to increase trust in use of edge resources? How would the CSA methodology need to change to support this type of assessment, and how useful is such an approach likely to be in practice? We propose a risk assessment methodology that can be used to address these concerns, and evaluate it in a practical application using both edge and cloud computing resources.

1. Introduction

Edge computing can be used to realise user requirements which have not been possible with cloud computing, such as pre-processing large data volumes closer to the generation source, ensuring personal data stays closer to the user and is not transferred over public networks to cloud providers. This also limits energy consumption of cloud providers, as data transfer from edge devices and computation at a data center can be minimised. The pervasive nature of edge devices also enables workload balancing, enabling excess tasks to be offloaded to a cloud platform (or vice versa – e.g. as identified in Osmotic computing[1]). Such mechanisms support coordination of resources (and associated tasks) with more intelligent access to edge resources especially when such resources are distributed [1].

The integration of edge resources with cloud infrastructures can be achieved through the use of an application-based orchestrator. It is important to iden-

[1] https://osmotic.org/

Preprint submitted to Elsevier *Received: date / Accepted: date*

tify resources that are part of such a federation, to ensure availability and a more informed task allocation to these resources [2]. Previous work [4, 22] has proposed edge-based orchestration for industrial processes on hardware/ system resources. The edge-orchestrator can be integrated with controllers and actuators to manage industrial processes in an energy management context.

We propose the use of an edge-orchestrator as a mechanism to support energy efficient task execution in a smart city context. Recent implementation of sustainable practices in cities and buildings requires a computational infrastructure that can sense, analyse and actuate based on signals received from resources and city *assets* [7]. Such sustainable interventions enable reducing carbon emissions by optimizing energy mix, improving the energy efficiency of equipment and machinery, and mitigating the environmental impact of resources [6]. This is the key contribution of this work, i.e. the implementation of an edge-orchestrator that is able to integrate resources across edge and cloud environments to achieve sustainable execution of tasks that have been generated from city-sensing and industry-based systems.

Industrial applications are adopting edge computing techniques to address data proximity requirements and a better orchestration of tasks for in-situ processing. Where edge and cloud resources are combined, it is important to identify where tasks can be deployed and potential reliability of edge infrastructure for executing a set of tasks [3] – this can use a utility-based model.

We introduce an *edge utility index* to federate edge and cloud infrastructure and utilise a methodology similar to the approach used by the Cloud Security Alliance (CSA) for certification of cloud providers based on their security credentials. The CSA approach uses a questionnaire that each provider needs to complete, and a cloud control matrix identifying a set of parameters to be considered as part of this questionnaire (covering storage, network, computational capacity etc). Our approach builds on this methodology to assess the *utility* edge resources offer to offload cloud services, taking account of energy efficiency and *competence* (the likelihood of successful completion of a task) of a resource. We evaluate our approach in an experimental test bed formed of RaspberryPi (RPi) controllers. An industrial application scenario is used to demonstrate the use of the approach in practice.

Specifically, we address the following questions: (i) how do we enable the formation of federated edge-cloud infrastructures to support execution of tasks within the edge? (ii) how do we allocate tasks in a federated cloud based on application requirements through the use of an orchestrator? The remainder of this paper is structured as follows: in section 2 we present related work in edge computing and integration of edge and cloud systems. In Section 3 we present our research methodology motivated by the CSA assessment methodology and how this can be extended with the use of am edge utility index. A number of scenarios are outlined in Section 4 to provide context and use of the proposed approach, followed by experimental results in Section 5. We conclude our work in Section 6.

2. Related Work & Requirements

The integration of edge and cloud systems has been extensively studied recently with the objective to scale applications and increase workflow performance [4, 5]. The dynamic integration of private/ public cloud systems with Internet of Things (IoT) devices can more efficiently accommodate different sets of task requests, as providers can cooperate by forming a *resource federation*, to enable resource sharing while addressing specific provider objectives. A federation in this context refers to integrating capacity across a number of different resources based on variation in demand [24]. To manage and create such resource federations, various game theoretic models can be adopted to provide more efficient use of resources [8]. A federation also enables integration of capability from multiple resource providers – limiting vendor lockin for a user and ensuring that a user is able to benefit from cost-benefit considerations across a number of different providers.

Integration of resources across both edge and cloud systems has been proposed to support data processing for IoT devices – based on a utility function that maximizes the number processing operations over a time window. Such utility based evaluation has shown to optimise the number of task requests that can be successfully executed. The edge nodes are coordinated by an *orchestrator* component (which may be hosted on the cloud platform or on an edge device) that also manages the interaction between different resources to execute application tasks [9]. To reduce latency in Cloud–IoT communications a secure cloud-to-edge middleware has also been proposed, supporting data confidentiality, integrity, authenticity and non-repudiation [10]. In heterogeneous cloud environments, resources can be grouped based on their capabilities (e.g. computational capacity), enabling identification of possible candidate resources for deploying tasks. Other heuristic approaches centered on the use of first-come-first-serve or best-fit approaches can also be used [22]. In this work we propose a utility-based orchestration strategy for deployment of tasks across edge and clouds resources.

The "Smartness Technology Readiness level" [11] agenda in Europe, focuses on the design of *sustainable interventions* for building assets, including energy efficiency and decentralisation of energy systems using green and renewable energy technologies. Such interventions involve the optimisation of energy supply with demand using storage, dispatchable generators, and a range of demand side management operating procedures [12]. This energy transition and smarter management of energy resources requires data processing capabilities which were *traditionally* provided via cloud systems – and which are now evolving towards the use of edge computing resources [13]. A key challenge is the development of the underlying computing infrastructure to select between potential interventions and coordinate their use.

Smartainability has appeared as a concept referring both to the "Smartness“ and "Sustainability“ of a city as a strategy to assess how sustainable smart cities are as a result of smart technology implementation [14, 15]. Such "smartainability“ refers to services and applications involving simulations, numerical modelling or optimisation and subsequent mechanisms for combining these. We leverage on such ”smartainability” approach and explore ways in which it can be achieved by including resilient and dynamically adaptive cloud and edge resources.

Supporting actuation and control of energy assets in sustainable cities also requires computational infrastructure that is able to respond to availability and distribution of renewable energy stock [16]. The development of smart energy systems in a city context needs to support: (i) a variation in energy demand that must be continuously optimised based on energy provision, (ii) the need for edge technologies to control and deliver distributed energy services, and (iii) an energy systems integration approach that provides a more informed management of the production of energy services, products and their distribution [17]. There are several open edge platforms that have been developed to support smart city services such as IOTech's Edge Xpert[2], Echelon SmartServer IoT platform [3] and JENEsys Edge [4]. Such platforms leverage on data collected from different sources to conduct analytics closer to the edge of the network i.e. sensor nodes [18]. Cloud computing is used for many smart city applications requiring intensive computing tasks whereby the IoT devices can support operations such as filtering, pre-processing and aggregating sensory data [19].

Existing smart cities applications have limited integration with recent generation of IoT systems – hindered by semantic interoperability of energy systems and limited semantic integration with urban artefacts, including prosumers, energy consuming devices / systems at building, district and wider city level. A more integrative smart city approach is needed to make more effective use of data generated by these different systems, and enable the use of deep learning/machine learning techniques adapted to the complexity of the urban energy landscape [20].

3. Conceptual Architecture

This section describes a conceptual architecture for integrating cloud and edge resources, based on the requirements identified in section 2. As shown in Figure 1, a cloud-edge federation architecture comprises of three layers, namely i) Cloud Layer, ii) Orchestration layer and iii) Edge resource layer. A brief description of these layers is as below.

- **Cloud layer** consists of traditional cloud computing platforms [26] hosted within managed data center(s). The cloud providers at this layer are said to have trust based collaborative relationship for sharing data and infrastructure with each other to form a horizontal federation. Each cloud provider has attained level-II certification from CSA i.e. the quantitative

[2] https://www.iotechsys.com/markets/industries/building-automation/

[3] https://www.dialog-semiconductor.com/products/industrial-edge-computing/smartserver-iot-edge-server

[4] https://www.lynxspring.com/technology

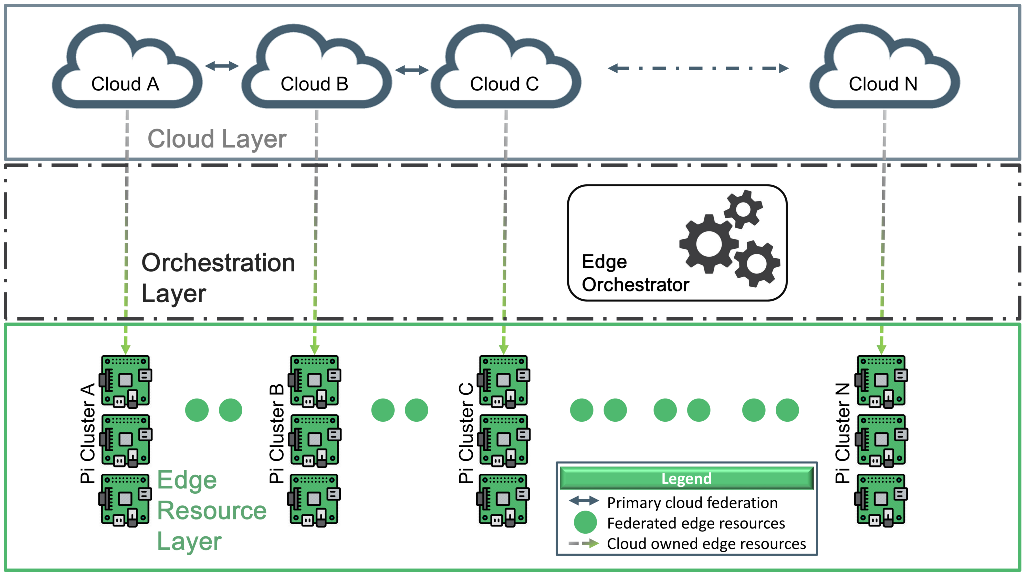

Figure 1: Cloud-Edge federation architecture

assessment of such Cloud Service Providers (CSP) is endorsed by CSA certified third party auditors.

- **Orchestration layer** consists of edge orchestrator (EO) [22] extended to act as a utility broker between the cloud and the edge layer thus facilitating the formation of dynamic cloud-edge federation. The utility function at the EO supports multi-criteria decision making based on static (Consensus Assessment Initiative Questionnaire (CAIQ)[5] based competence assessment) as well as dynamic (performance) indicators. The static indicators are mostly used as a bootstrap mechanism for newly joining CSPs with no previous history of interaction and performance data.

- **Edge resource layer** consists of edge IoT devices (e.g. a Raspberry Pi (RPi) or an NVidia Jetson) owned by their respective cloud provider but are located in-proximity to the data source. Compared to cloud-based systems, these devices have limited computational and data storage capacity and therefore may be combined together into an edge cluster to execute user tasks.

The above mentioned federation has been deployed on edge and cloud systems, with five Raspberry Pi 3 (Model B) nodes and five HPC nodes in our testbed. Each Raspberry Pi 3 supports a Quad Core 1.2GHz Broadcom BCM2837

[5] https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-1/ – released in April 2020

with 64bit CPU 1GB RAM, BCM43438 wireless LAN and Bluetooth Low Energy (BLE) on board 100 Base Ethernet 40-pin extended GPIO. A Micro SD card is used for loading the operating system and storing necessary data. The experiments are developed around two types of resources:(i) cloud resources located at multiple network hops from the data source, and (ii) edge resources which are located within proximity of the data source, i.e. within the factory.

3.1. Cloud Security Allience (CSA) STAR program

A "Security, Trust & Assurance Registry (STAR)" program [21] has been proposed by Cloud Security Alliance (CSA) that aims to provide transparency in assessing cloud providers based on their security capability. CSA STAR is a three level program offering a publicly accessible STAR registry containing data regarding assessment of more than 200 cloud providers. At level-I, it allows providers to publish self-assessment of their security controls, in the form of a standardized "Consensus Assessments Initiative Questionnaire (CAIQ)". At level-II, an independent third party audit is made for CAIQ attestation and certification of the cloud provider. At level-III, a mechanism for certification based on continuous monitoring is proposed [21] with the aim to provide assessment and compliance on a continuous basis. This data can be retrieved, analysed and used in a variety of contexts by customers and software (tool) vendors.

- *Cloud Control Matrix (CCM)*: As a part of the CSA STAR program, CCM delivers a framework for assessment of security capabilities of a cloud provider, providing controls over 16 domains. These domains and their respective controls enable cloud providers to present their capabilities related to security and privacy. A series of questions made available in the CAIQ can be used by third party organisations to attest (verify) these capabilities. The foundations of CCM is based on other industry-accepted control frameworks and security standards, e.g. ISACA, PCI, NIST, ENISA, COBIT, ISO 27001/27002, NERC CIP and Jericho Forum etc. CAIQ can be used by cloud providers to reveal their security and privacy capabilities to customers in a standardized and consistent way. However, as this process is a self-assessment, customers/ users may require further evaluation by an independent and trusted third-party organization.

- *Consensus Assessment Initiative Questionnaire (CAIQ)*: Based on CCM, CAIQ offers a method to assess the competencies and capabilities of providers for different attributes i.e., compliance, governance, security etc. Despite heterogeneity in infrastructures, this standard method of demonstrating capabilities allows a client or a user to analyse, compare or combine information from multiple CSPs over a homogeneous parameter space. The outcome of CAIQ assessment supports clients for informed decision making well before contracting a provider in a case when there is no availability of historical performance ratings (i.e. the provider is new in the market) or given there is a possibility for biased feedback or false ratings (provider collusion). Afterwards, the relationships can be viewed or monitored during actual service enactment. CAIQ assessment information can therefore be used for both skilled as well as new entrants to the cloud marketplace. CAIQ contains a set of 295 assertions that a provider (or an auditor) answers as either yes, no or not applicable. These assertions are categorized into 133 control groups and 16 control domains grouped by their relevance as in CCM and are shown in Table 1.

3.2. Proposed method of mapping CAIQ and CCM

This approach proposes to adapt the relationship between CAIQ and CCM to support edge-cloud resource federation. This relationship can be used to evaluate the capability of a resource based on the type of service for which that resource is used. Mapping CCM with CAIQ provides us various controls that can be considered in a specific context. We propose considering a specific set of control assertions which are specifically applicable for the specific case of edge clusters. Referring to Table 2, it can be observed, for example, that the total number of questions in 'Datacenter Security' control domain is 11, however, only 5 out of these 11 are deemed relevant for an edge cluster – as explained further in subsequent sections.

Table 1: Nomenclature of CCM/CAIQ and proposed applicability to edge cluster

			Total	Total	Relevant questions to
No.	ID	Control Domain	controls	questions	Edge cluster
		(16)	(133)	(295)	(245)
1	AIS	Application & Interface Security	4	9	9
2	AAC	Audit Assurance & Compliance	3	13	13
3	BCR	Business Continuity Management & Operational Resilience	11	22	17
4	CCC	Change Control & Configuration Management	5	10	10
5	DSI	Data Security & Information Lifecycle Management	7	17	15
6	DCS	Datacenter Security	9	11	5
7	EKM	Encryption & Key Management	4	14	14
8	GRM	Governance and Risk Management	11	22	12
9	HRS	Human Resources	11	24	14
10	IAM	Identity & Access Management	13	40	37
11	IVS	Infrastructure & Virtualization Security	13	33	33
12	IPY	Interoperability & Portability	5	8	6
13	MOS	Mobile Security	20	29	17
14	SEF	Security Incident Management, E-Discovery, & Cloud Forensics	5	13	13
15	STA	Supply Chain Management, Transparency, and Accountability	9	20	20
16	TVM	Threat and Vulnerability Management	3	10	10

4. Edge Utility Index for Cloud-Edge Federation

We consider a "vertical federation" formed between a CSP and edge resources that are present at the edge layer. The EO plays an important part in the formation of such cloud-edge federation by acting as a mediator between the two layers. The EO evaluates the Edge Utility Index (EUI) of each virtual edge resource using the capability and competence of the cluster. A CCM/CAIQ mapping based assessment approach has been adapted for use with edge-cloud resources that may be limited in their capacity of resources but share the same nomenclature as that of cloud service providers. The requisite control domains and control questions applicable to the virtual edge resource is given in Table 1. The competence of an edge resource is based on its performance in previous projects and the number of successfully completed tasks within these projects.

4.1. Methodology

The *EO* (described in section 3) is responsible for calculating the EUI value as illustrated in Figure 1. In the proposed approach, we have used various key operators as defined in Table 2.

Table 2: Quantitative parameters of proposed research

Metric	Parameter	Description
Capability	Positiveness	Average +ve declarations by a CSP
	Negativeness	Average -ve declarations by a CSP
	Belief	Expectation based on positiveness
	Disbelief	Expectation based on negativeness
	Uncertainty	Uncertainty in expectation
	Initial expectation	Prior knowledge of +ve/-ve expectations
Competence	Job Type	Nature of job assigned to the nodes
	Data Size (MB)	Size of the job in storage
	Tasks	No. of tasks in given job type
	Completion Time	Time to completion (seconds)
	Task delivery ratio	A ratio representing success or failure rate
Decision	Perceived Capab.	Audit-based Security capab.
	Perceived Compet.	No. of tasks performed per second
	Aggregated Compet.	Aggregated competence over n prev. tasks
	Importance	Current benefit of including a resource

Following a request for adding a new edge cluster to the federation (project), a *add_new_resource* message is sent to the *EO*, with the required *utility_criteria*. A list of virtual resources having EUI matching the *utility_criteria* is forwarded to the requesting entity. Afterwards, any further decision for final selection of the resource can be made, following which the *EO* initiates the requisite process to engage the given device as part of the federation.

At the start of this process and to become eligible as a participant of the federation, an edge cluster must possess a valid set of CAIQ assessment. This assessment must fulfil the criteria as recognized by CSA, along with relevant certifications for these criteria. This CAIQ assessment is parsed to get *capability_metric* required by the 'EUI Evaluation' function. This function supports a numerical representation of the *capability* of the given edge device and stores it in a repository for further evaluation of EUI. The details of evaluating *capability* is further discussed in section 4.2.

Afterwards, an edge device can take part in the federation to process the assigned tasks as per given criteria in a request. The *competence* achieved by performing these tasks is then evaluated along with the *importance* of the cluster in terms of task delivery ratio as a part of *competencemetric*. Details regarding concepts of *competence* and *importance* can be found in section 6.1 and 6.2 respectively. Using both these metrics for an edge device x, to be included in federation for a task 'α', given a context of use c, the EUI is given as:

$$EUI(x, \alpha, c) = \sum_{i}^{c} \left(\frac{Perceived\ Capability(x, \alpha, c)}{Aggregated\ Competence(x, c)} \times I(x, \alpha, c) \right) \tag{1}$$

given $Perceived\ Capability(x, \alpha, c)$ and $Perceived\ competence(x, c)$ of an edge resource x based on respectively on its CAIQ assessment and performance as monitored by EO. In equation 1, $I(x, \alpha, c)$ denotes the importance of introducing a given edge resource (for any context c) dependant on its task delivery ratio. These parameters collectively makes up the profile of an edge resource registered with the EO. Initially, when a device becomes a part the federation and has no historical performance ratings available, its profile is only based on the CAIQ evaluation and its acquired certification level known collectively as its *capability.* The details of evaluating all parameters is given in the sections below.

4.2. Edge Capability

The *edge_capability* reflects the ability of a resource to conform to CSA certification. This compliance must relate to a particular context of any given project collaboration, e.g. considering a resource acting as a 'storage' repository within a federation requires that this resource should be evaluated only on the basis of CAIQ assertions requisite to storage. In this way, CAIQ assessment can be limited to only relevant controls for this specific service provisioning instead of all controls. In the case of edge cluster, we propose to only consider control assertions as mentioned in table 4.2 relevant to the resource capabilities.

For edge capability evaluation, the approach discussed in [23, 24] for cloud federation has been extended to represent each capability domain as an opinion of an edge cluster towards its security and privacy settings. This opinion is a collective view of CSP's answers to assertions of CAIQ, whether positive or negative, and known as 'declarations'. Each positive answer *'p'* to an assertion reflects the presence of an attribute and marks an increase in the belief (λ) on the edge capability. Whereas, a negative answer *'q'* adds to the average negativeness of the domain and adds to the disbelief (γ) on that resource's capability. An unanswered assertion 'un' is counted towards an increase in uncertainty (φ). The derived opinions are afterward stored in the repository for further evaluation to derive *'Perceived Edge Capability'* decision operator as and when required. Considering a specific context of edge cluster given p as the total number of positive and q as total number of negative declarations along with un being *unanswered* and NA being *not applicable* declarations along with $N = (p + q + un)$ depicting the total applicable assertions as given in 4.2 for an edge cluster context, the capability of an edge resource can be evaluated as:

$$T(\lambda, \gamma, \varphi, \epsilon) = \lambda + \varphi * \epsilon \tag{2}$$

given

$$\lambda = \rho * \zeta; \gamma = \eta * \zeta; \varphi = 1 - \zeta; \tag{3}$$

$$\rho = \frac{p}{p+q}; \eta = \frac{q}{p+q}; \zeta = \frac{N*(p+q)}{2*(N-p-q)+N*(p+q)}; \tag{4}$$

In equation 3, λ, γ and φ represents the belief, disbelief and uncertainty associated with the cluster capability respectively. ρ and η are the average positiveness and average negativeness of a domain respectively based on p and q for each domain. Confidence ζ, is based on p and q, along with $N = (p+q+un)$ and an initial expectation of $\epsilon = 0.99$ for optimistic evaluation. A cumulative edge capability score C of a resource is achieved by aggregating opinions of all control domains related to the edge resource as given in table 4.2.

Table 3: Individual capability representation of five different edge clusters

Edge Resource	N	p	q	un	λ	γ	φ	C
A	245	230	15	0	0.9388	0.0612	0	0.9388
B		163	82	0	0.6653	0.3347	0	0.6653
C		161	31	53	0.8367	0.16114	0.0022	0.83888
D		98	85	62	0.534	0.4632	0.0028	0.53677
E		196	12	37	0.9409	0.05761	0.0015	0.94239

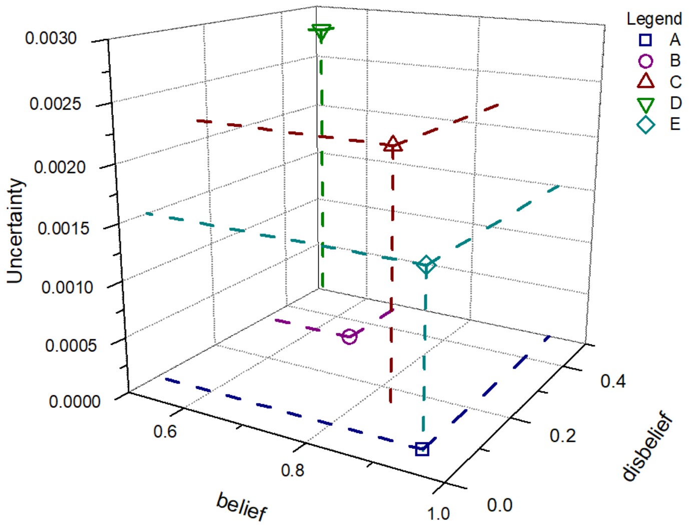

Figure 2: A 3-Dimensional representation of capability scores of virtual edge resources

Using equations 2-4, Table 3 shows N, p, q and un scores evaluated from the CAIQ data retrieved from CSA STAR repository. The repository consist of CAIQ data set corresponding to cloud providers, and the same has been retrieved for five random providers having level-II certification. Afterwards, referring to table 2, control relevant to five random Pi clusters, for example, A, B, C, D and E, are retrieved for further processing.

The values of p and q represent the total number of positive and negative answers respectively, whereas values of un represent questions left unanswered by the provider. These three values must aggregate as the total number of applicable assertions N i.e. 245 in case of edge resource. The capability parameters i.e. belief, disbelief and uncertainty are represented in Figure 2 for all resources along X-axis, Y-axis and Z-axis respectively. Among all these given resources, E is seemingly rated the best for having the maximum capability value. However, resource E having uncertainty in its evaluation can not be considered best for federation. This makes the resource A as the possible choice among all resources.

5. The smart city scenario

We deploy our model within a fish processing factory located in the port of Milford Haven [25]. The fish processing site consists of five major buildings – labelled F, J, K and M sheds along with a main Packaway building (see Figure 4). Each building owns a set of PV panels for energy production and a number of energy consuming appliances used for fish processing. Each building is coordinated by an edge layer for of each devices that controls the operation via actuation setpoints implemented periodically.

The key objective is to develop a "smart port capability" that can enable sustainable interventions at the port level based on a wide range of IoT/edge technology involving remote sensing, monitoring and actuation of essential assets. The implementation of the smart port aims also to improve the failure response times and ensure more predictability around asset availability.

We conduct experiments on the main Packaway Building that contains several energy-consuming appliances i.e. lighting systems and smart meters along with a box washing machine, a flake ice machine and an ice store freezer. The Packaway Building has a washing machine that operates only when the fishermen has to clean their boxes during the day. Total energy consumption of this machine is approximately 50 kW. The ice flake machine operates all day to cater for the ice quantity required for fish storage. Each appliance is controlled by a RaspberryPi3 forming an edge environment within the building.

5.1. Edge controllers scenario

The Packaway building has numerous appliances that are monitored by smart meters and are controlled by Raspberry Pis' that consumes energy coming from the local PV units or the main power grid. In order to explore the mechanisms involved in the deployment of an industrial edge network, we consider the following consumption units:
Edge consumption units:

- *Ice Flake machine* – The ice flake system is operational all day and consumes energy according to different operating schedules in relation to the daily fish processing demand.

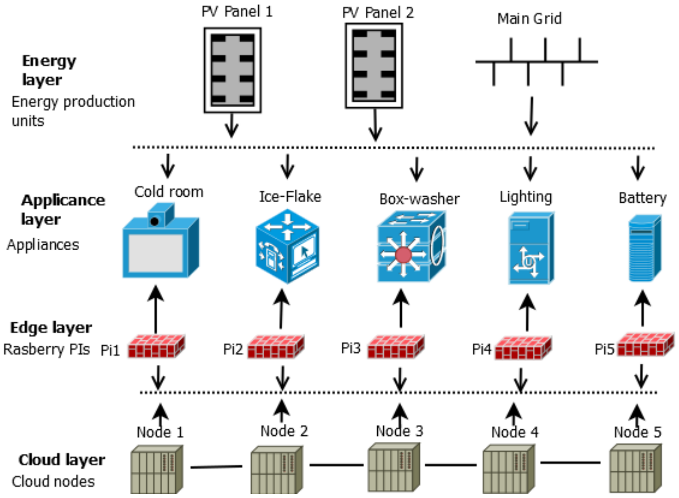

Figure 3: Edge layer in a smart port scenario

- *Cold room* – The cold room is an appliance in the building having a high power consumption. The cold room has a temperature set-point and an operating schedule which has a direct impact on the energy consumption by the appliance.
- *Box washing machine* – This machine consumes a total of 50 kWh and usually works on a very limited daily interval, hence the power consumption is low.
- *Lighting* – The system used for lighting this building is only used during the night and consist of approximately 23 double tubes lights of 25W each. Each storage room (total 4) in the Packaway building has a double tube lighting system.

Edge production units has (i) local PV systems with 50kW panels for each building and (ii) a 5MW solar farm containing approximately 20,000 panels. All consumption units are monitored by smart meters and controlled by RPis that host intelligent optimisation algorithms. The actuation implemented by the RPi into an appliance takes into account the following objectives:

- *Reducing energy consumption* – the main objective is to provide greater efficiency and more informed usage of energy in the local industrial site and wider within the community.
- *Managing energy production* – The objective is to enable energy producers to have more control over their production sources and to decentralise production at both the site level and the community level.

We record setpoints values from the appliances such as box-wash, ice flake machine, cold-room temperature setpoint and lighting. These setpoint values are measured every 15 minutes and used as input variables in the simulation scenario. All sensors and devices are non-invasive.

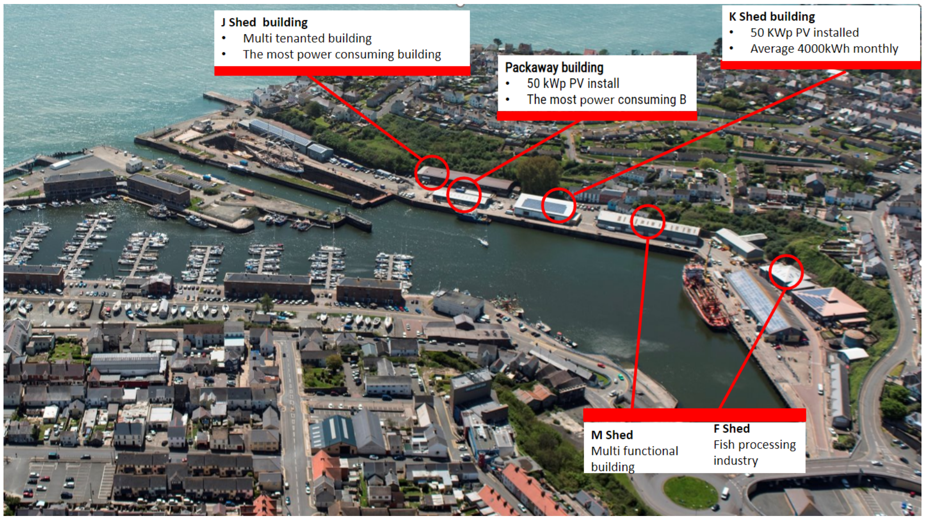

Figure 4: Overview of the Milford Haven port

In the Milford Haven port, houses located in proximity of the marina are used as living areas for staff working at the port. There are 200 houses with different energy loads, in the process of being modified to support energy management involving automation and integration of renewable. A possible application is to scale our federation model across all buildings to achieve integration and sustainable interventions at the level of an entire community. This involves replication of the proposed edge and cloud federation with a view to integrate consumption and production units such as energy consumption (load profile), PhotoVoltaic (PV) generation, battery/storage systems management, and connection to the energy grid. The smart port would provide a more informed management of the load status, energy generation by the PV system, grid exchange, and the storage system including use of battery-powered and electric vehicles (including electric boats).

6. Experiments

The proposed model has been evaluated based on experiments considering the following objectives:

- Evaluate the effectiveness of the federation manager in aggregating cloud and edge nodes. This includes the following considerations: (i) use no edge resources; (ii) use cloud+edge resource together; (iii) multiple edge resources – select which ones to use in the federation. How effective is the use of perceived competence as a measure to select resources?

- Compare with performance evaluation carried out in [22] where the key focus was on job execution using EO, and the jobs were diverted to run either on edge or cloud resources based on properties of the job. A key consideration is how effective is the use of a federation manager vs. a random allocation to resources [22].

6.1. Aggregated Competence

The *aggregated_competence* metric relates to the accumulated performances of a resource over a finite period of time. Each performance is measured as *perceived_competence* for every task that the resource has performed. Given a set of jobs j e.g. as in table 4, the perceived competence of an edge cluster is time metric given as,

$$perceived\ competence = \frac{total\ time\ taken\ by\ a\ job}{number\ of\ tasks\ in\ a\ job} \tag{5}$$

For example, given a JobType3 with 32 tasks takes an edge device 160 seconds to process, this gives us a perceived competence of 5s/task. Taking only the latest value of the competence may not fully reflect resource behaviour, therefore historical values of perceived competence must be taken into account. One way to do this is to have an aggregated effect as a mean of all values from competence calculations of previous projects. However, recent competence must have a clear advantage over previous ones. Moreover, historical performance may not be an effective indicator of current and future behaviour. In order to reduce the impact of previous performance, we propose to aggregate the previous performances such that recent performance has greater effect on the competence of the cluster. Given N as the total number of previous (historical) performance values to be taken into account, aggregated competence can be evaluated as:

$$\sum_{n=1}^{N} comp = \omega * comp(N) + (1-\omega) * \sum_{n=1}^{N-1} comp \tag{6}$$

where ω is a decay function given as

$$\omega = (1 - \frac{1}{N})^{n} \tag{7}$$

thus giving more weight to the recent competence instead of just averaging all available values as illustrated in Figure 5. This figure depicts the comparison of individual competence values with simple averaging and proposed aggregated competence mechanism for N=5 and 10 for a random edge resource. As evident from the figure, simple average is least representative of the current competence value.

6.2. Importance

The significance of an edge resource for contributing to the federation is given by its importance I. Task delivery ratio is a useful indicator of the overall

Table 4: Job Information

JobType	Data Size (MBs)	Tasks
JobType1	50	16
JobType2	100	24
JobType3	150	32

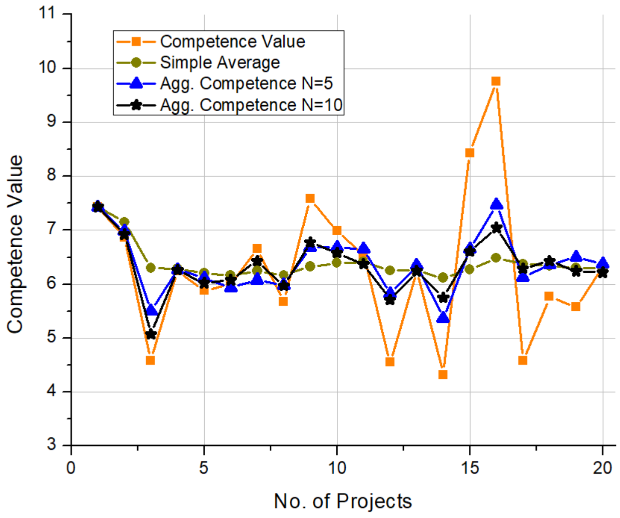

Figure 5: Effect of decay on aggregated competence in case of N=5,10 as compared to simple average

Importance of a device within the federation. In order to stop malpractice of task over bidding in the federation, the importance of a device is given by:

$$importance(I) = \frac{s}{s+f} \tag{8}$$

$$s = number\ of\ successful\ tasks, f = number\ of\ failed\ tasks \tag{9}$$

Any resource can gain back its importance value with the passage of time only with increase in the number of successful tasks. Figure 6 represents the variation in importance of three different edge resources namely A, B and C respective to their variation in success rate. The resource A depicts an ideal scenario of importance due to its high success rate, as compared to B and C. Resource B is depicted to lose its importance due to periodic failures to complete its designated tasks. However, resource B, having its success rate greater than the failure rate, managed to eventually gain its importance. Resource C is depicted to have intermittent success and failure at the task delivery, thereby

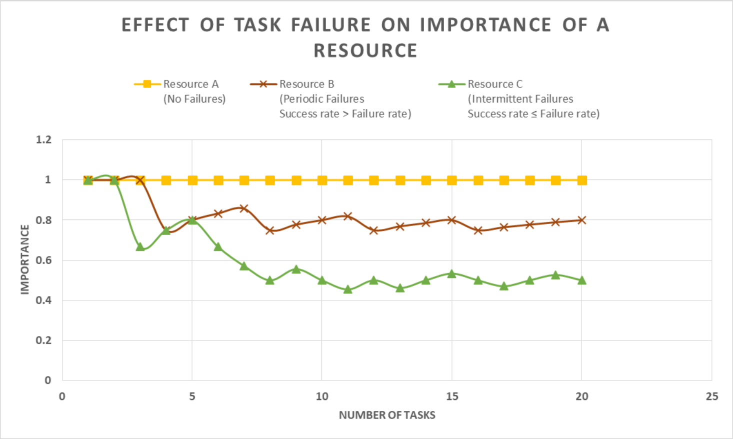

Figure 6: Importance of resource A, B and C in relation to their failure rates

having a fluctuating importance, which eventually fails to recover with the passage of time.

7. Conclusions

Increasing availability of edge computing resources enables these to be used alongside cloud systems for executing user applications. Edge computing resources however can differ in their capability, security and availability profiles – making reliance on them risk prone. We describe how a federated edge-cloud infrastructure can be realised using a similar assessment strategy as adopted by Cloud Security Alliance using CAIQ/CMM for combining capability across these two groups of resources.

We also describe how federated resources across edge-cloud can used to support energy forecasting and scheduling for the fish processing industry at the Milford Haven port in the UK (one of the largest such facilities in Europe). The proposed approach can be generalised across a number of other similar applications, such as sensing energy use within buildings within a city, in addition to the use of renewal energy sources (such as PV panels – also considered in our scenario).

The instrumentation of recent smart cities applications is primarily developed around sensors and controllers and smart devices. We present a model of how such devices can be integrated to support the sustainable interventions for cities. We show how trust can be established across an ensemble of ”smart” devices and clouds to support ”risk-informed” interventions. Our assumptions combine the computational layer with the operational layer identified in a smart city scenario (i.e. smart port), to demonstrate how edge-cloud federation can incentive and advance sustainability for buildings, infrastructures and cities.

The approach proposed in this paper demonstrates how edge-cloud infrastructures can be federated to support industrial workflows with a key emphasis on security and competence. We address the security implications of such edge-cloud federation by also using the Cloud Security Alliance methodology where resources are assessed prior to the formation of the federation. Our results show that perceived competence of edge/cloud resources are important when forming a federated ecosystem especially when resources can have different availability and capacity constraints. We also associate an index with an edge resource to assess its suitability for being integrated into a resource cluster comprising edge and cloud resources.

Declaration of Competing Interest The authors declare that they have no known competing financial interests. All authors have read the manuscript and have approved this submission.

Acknowledgements This work uses scenario data from the EU INTERREG piSCES project, grant number 504460. We thank Ateyah Alzahrani for sharing an illustration of the Milford Haven port.

References

[1] Liu, Lumin, et al. "Client-edge-cloud hierarchical federated learning." IEEE International Conference on Communications (ICC). IEEE Computer Society Press, 2020.

[2] Xu, Xiaolong, et al. "A computation offloading method over big data for IoT-enabled cloud-edge computing." Future Generation Computer Systems 95 (2019): 522-533.

[3] Lin, Fuhong, et al. "A novel utility based resource management scheme in vehicular social edge computing." IEEE Access 6 (2018): 66673-66684.

[4] Petri, I., Zamani, A.R., Balouek-Thomert, D., Rana, O., Rezgui, Y. and Parashar, M., 2018, December. Ensemble-based network edge processing. In 2018 IEEE/ACM 11th International Conference on Utility and Cloud Computing (UCC) (pp. 133-142). IEEE.

[5] I. Petri et al., "Cloud Supported Building Data Analytics," 2014 14th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 2014, pp. 641-650, doi: 10.1109/CCGrid.2014.29.

[6] N. B. Ahamad, M. Othman, J. C. Vasquez, J. M. Guerrero, C.-L. Su, Optimal sizing and performance evaluation of a renewable energy based microgrid in future seaports (2018) 1043–1048.

[7] I. Petri, O. Rana, L. F. Bittencourt, D. Balouek-Thomert and M. Parashar, "Autonomics at the Edge: Resource Orchestration for Edge Native Applications," in IEEE Internet Computing, doi: 10.1109/MIC.2020.3039551.

[8] Farris, I., Militano, L., Nitti, M., Atzori, L. and Iera, A., 2017. MIFaaS: A mobile-IoT-federation-as-a-service model for dynamic cooperation of IoT cloud providers. Future Generation Computer Systems, 70, pp.126-137.

[9] Farris, I., Militano, L., Nitti, M., Atzori, L. and Iera, A., 2015, December. Federated edge-assisted mobile clouds for service provisioning in heterogeneous IoT environments. In 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT) (pp. 591-596). IEEE.

[10] Celesti, A., Fazio, M., Galletta, A., Carnevale, L., Wan, J. and Villari, M., 2019. An approach for the secure management of hybrid cloud–edge environments. Future Generation Computer Systems, 90, pp.1-19.

[11] EU Comission, Smart Readiness Indicator for Buildings, available at: https://smartreadinessindicator.eu/, Last accessed: August 2021

[12] Ahad, Mohd Abdul, et al. "Enabling technologies and sustainable smart cities." Sustainable cities and society 61 (2020): 102301.

[13] Bisello, Adriano, and Daniele Vettorato. "Multiple benefits of smart urban energy transition." Urban energy transition. Elsevier, 2018. 467-490.

[14] Giffinger R, Fertner C, Kramar H, Kalasek R, Pichler-Milanovic N. Smart cities – Ranking of European medium-sized cities. Final report. Centre of Regional Science, Vienna UT, 2007. www.smart-cities.eu

[15] Giacomello L, De Benedetti B, Tecchio P, Rollino S. Life Cycle Assessment of sustainable home gateways and product category rules definition for environmental labelling. Politecnico di Torino, DISAT – Dipartimento Scienza Applicata e Tecnologia, 2013. www.disat.polito.it.

[16] Petri, Ioan, et al. "Federating smart cluster energy grids for peer-to-peer energy sharing and trading." IEEE Access 8 (2020): 102419-102435.

[17] Liu, Yi, et al. "Intelligent edge computing for IoT-based energy management in smart cities." IEEE network 33.2 (2019): 111-117.

[18] A. Sharma, A. S. Sabitha, A. Bansal, Edge analytics for building automation systems: A review, in: 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), IEEE, 2018, pp. 585–590.

[19] L. U. Khan, I. Yaqoob, N. H. Tran, S. A. Kazmi, T. N. Dang, C. S. Hong, Edge-computing-enabled smart cities: A comprehensive survey, IEEE Internet of Things Journal 7 (2020) 10200–10232

[20] Reynolds, J., Rezgui, Y. and Hippolyte, J. 2017. Upscaling energy control from building to districts: current limitations and future perspectives. Sustainable Cities and Society 35, pp. 816-829. (10.1016/j.scs.2017.05.012)

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

[22] I. Petri, O. Rana, A. R. Zamani, and Y. Rezgui, ”Edge-Cloud Orchestration: Strategies for Service Placement and Enactment,” in 2019 IEEE International Conference on Cloud Engineering (IC2E), 2019, pp. 67-75.

[23] U. Ahmed, I. Petri, O. Rana, I. Raza, and S. A. Hussain, ”Risk-based Service Selection in Federated Clouds,” in 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), 2018, pp. 77-82.

[24] U. Ahmed, I. Petri, O. Rana, I. Raza, and S. A. Hussain, ”Federating Cloud Systems for Collaborative Construction and Engineering,” IEEE Access, vol. 8, pp. 79908-79919, 2020.

[25] Alzahrani, A., Petri, I. and Rezgui, Y. 2020. Analysis and simulation of smart energy clusters and energy value chain for fish processing industries. Energy Reports 6(S1), pp. 534-540. (10.1016/j.egyr.2019.09.022)

[26] P. Mell and T. Grance, ”The NIST definition of cloud computing,” NIST, USA 800-145, 2011.