Context-aware IoT-enabled Cyber-Physical Systems: A Vision and Future Directions

Karan Mitra[1], Rajiv Ranjan[2], and Christer Åhlund[1]

[1] *Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Skellefteå, Sweden. Email: [karan.mitra,christer.ahlund]@ltu.se*

[2] *School of Computing, Newcastle University, Newcastle upon Tyne, United Kingdom. Email: raj.ranjan@ncl.ac.uk*

Abstract

The next-generation cyber-physical systems (CPSs) will not only be limited to industries but will span across multiple application-areas regarding smart cities and regions. These CPSs will leverage the recent advancements in the areas of cloud computing, Internet of Things and big data to provision citizen-centric applications and services such as smart hybrid energy grids, smart waste management, smart healthcare and smart transportation. Challenges regarding context-awareness, quality of service and quality of experience, mobility management, middleware platforms, service level agreements, trust, and privacy needs to be solved to realize such CPSs. This chapter discusses these challenges in detail and proposes ICICLE - a context-aware IoT-enabled cyber-physical system as a blueprint for next-generation CPSs.

1 Introduction

Cyber-physical systems (CPSs) tightly integrate computation with physical processes [6]. CPSs encompass computer systems including physical and virtual sensors and actuators connected via communication networks. These computer or *cyber systems* monitor, coordinate and control the physical processes, typically via actuators, with possible feedback loops where physical processes affect computation and vice versa [6]. CPSs are characterized by stability, performance, reliability, robustness, adaptability, and efficiency while dealing with the physical systems [41, 27].

CPSs are typically associated with tightly-coordinated industrial systems such as manufacturing [27, 42]. Currently we are at the cusp of witnessing the next generation CPS that not only span industrial systems, but also include wide application-areas regarding smart cities and smart regions [5]. The next generation CPSs are expected to leverage the recent advancements in cloud

computing [21], Internet of Things (IoT) [13], and big data [44, 8] to provision citizen-centric applications and services such as smart hybrid energy grids, smart waste management, smart transportation, and smart healthcare IoT. [13] has emerged as a new paradigm to connect objects such as sensors and actuators to the Internet to provide services in the above mentioned application areas.

Big data is referred to as data that cannot be processed on a system under use [44]. For example, a Boeing aircraft engine produces ten terabytes of data every thirty minutes. This data cannot be processed on a typical mass-produced desktop and laptop, and therefore considered as big data. Cisco predicts that by the year 2020, there will be fifty billion devices connected to the Internet[1]; in the year 2021, 847 zettabytes of data will be produced by IoT applications[2]. Big data can be *valuable* if we can efficiently use raw sensor values (which are often misunderstood, incomplete and uncertain [30]) or *context attribute values* [3] to determine *meaningful information* or *real-life situations.* This necessitates the development of novel context-aware systems that harness big data for context-aware reasoning in a CPS. Context-aware systems provide methods to deal with raw sensor information in a meaningful manner under uncertainty and provide mechanisms for efficient context collection, representation and processing. Big data context reasoning may require the use of a large number of computational and software resources such as CPU, memory, storage, networks, and efficient software platforms to execute data processing frameworks such as MapReduce.

The cloud computing paradigm enables provisioning of highly available, reliable, and cheaper access to application (such as big data applications) and services over the network. National Institute of Standards and Technology (NIST) define cloud computing as [21]: *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

Cloud computing is characterized by [21]: *on-demand self service* where cloud resources such as compute time, memory, storage and networks can be provisioned automatically, without human intervention; *broad network access* ensures that the cloud resources are provisioned over the network and can be accessed by myriad devices including smart phones, tablets, and workstations; *resource pooling* is the ability to share cloud resources with multiple customers at the same time; this is achieved via virtualization where cloud (physical) resources are partitioned into multiple virtual resources [3]. These virtualized resources are then shared with multiple users using the multi-tenant model. Based on the usage of these resources, the customer is charged on pay–as-you-go basis;

[1] https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [Online], access date: 2 July 2020

[2] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html#_Toc503317525 [Online], access date: 8 June 2020.

[3] A context attribute is the data element at a particular time instance that is used to infer a real-life situation(s) [30].

rapid elasticity is the ability of the system to scale out (add resources) or scale in (release resources) based on the demands posed by application and services workloads. Elasticity is one of the definitive property of cloud computing as it gives the illusion of infinite capacity to the customers; *measured services* ensure transparency for both the provider and the customer as the resource usage can be monitored, metered and logged that can be used for resource optimization and billing.

A recent joint report from NICT and NIST [37] aims to define an integrated cyber-physical cloud system (CPCC) to develop a robust disaster management system. This report defines CPCC as *"a system environment that can rapidly build, modify and provision auto-scale cyber-physical systems composed of a set of cloud computing-based sensor, processing, control and data-services"*. The report argues that IoT-based cyber-physical cloud system may offer significant benefits such as ease of deployment, cost efficiency, availability and reliability, scalability, ease of integration [37]. Xuejun *et al.* [41] and Yao *et al.* [42] assert the need to harness the recent advances in the areas of cloud computing, IoT, and CPS and integrate them to realize next-generation CPS. Therefore, the overall aim of an IoT-based cyber-physical system would be an efficient integration of cyber objects with cloud computing to manage physical processes in the real world.

This chapter proposes ICICLE: A Context-aware IoT-based Cyber-Physical System that integrates areas such as cloud computing, IoT, and big data to realize next-generation CPS. This chapter also discusses significant challenges in realizing ICICLE.

2 ICICLE: A Context-aware IoT-enabled Cyber-Physical System

Figure 1 presents our high-level architecture for context-aware IoT-based cyber-physical system. The figure shows the cyber and physical systems and the interaction between them. The cyber system consists of the cloud infrastructure hosting software components such as those related to context collection, processing and reasoning, and application monitoring. The physical system involves IoT devices such as sensors and actuators that are connected to cyber systems via IoT gateways or directly. We now discuss ICICLE in detail.

Devices/Things: The IoT application components, the network, and the cloud form the cyber part of the system, whereas, the sensors and actuators constitute the physical part of the system as they are responsible for sensing the environment and controlling the physical processes. As we expect a large number of IoT devices to be deployed in application areas regarding smart cities, it is highly likely that many of these devices may produce a similar type of data. For example, outside temperature sensors placed on the lamp posts, on public and private buildings produce temperature data. The raw data sensed and collected from these devices can be used to determine the temperature

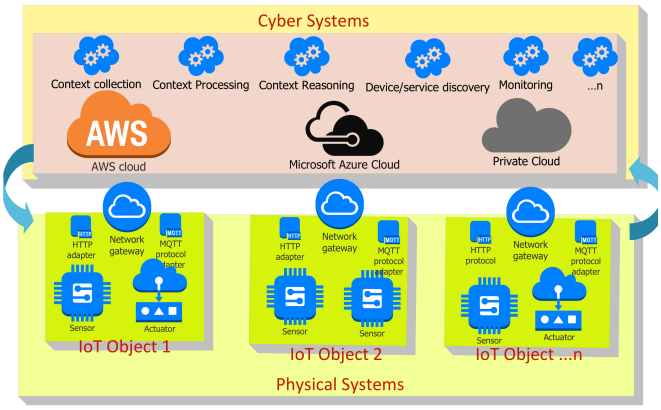

Figure 1: ICICLE: Context-aware IoT-enabled Cyber-Physical System.

at the same location, such as, for a particular suburb; these sensors can also be clubbed together to formulate a virtual IoT device that can be integrated as part of ICICLE as a cyber component. It is important to note that virtual sensors may also encompass information for various sources such as online social networks (e.g., Facebook and Twitter) [37], as well as open data published by governments, municipalities, as well as industries. In ICICLE, the IoT devices may connect to a gateway or directly to the Internet via multiple access network technologies such as WiFi, ZigBee, LoRaWAN, GPRS, and 3G. Further, the IoT devices may use a wide variety of application layer protocols such as HTTP, CoAP, MQTT, OMA Lightweight M2M, XMPP, and WebSocket [4, 14]. For each application layer protocol, there are plugins deployed at the sensor/gateway and the applications running in the clouds. The plugins encode and decode the sensor data as per requirements.

Services: The data collected from the IoT device is sent to the cloud datacenters for processing and storage. The data retrieval from the IoT devices can be both pull and push-based and can also be done via the publish-subscribe system [4]. In the pull-based approach, the IoT devices themselves or they connected via the gateway can offer an endpoint (via uniform resource locator (URL) or directly via an IP address) for data access. The applications (standalone applications, middleware such as FIWARE[4], and virtual sensors) can then fetch the data directly from the endpoint. In the push-based approach, the data can be sent directly from the IoT devices/gateway to the applications hosted on the clouds. In the publish-subscribe system, an entity-broker is involved. The IoT device/gateway sends the data to the topics managed by the

[4]http://www.fiware.org. Access date: 19th June 2020.

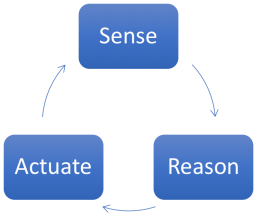

Figure 2: Steps to achieve context-awareness.

broker. As soon as the IoT device/gateway sends the new data to the broker on a specific topic, the broker publishes the data and send it to the subscribing applications or the virtual sensors.

Context-awareness: ICICLE considers context-awareness as the core technology that enables operational efficiency and intelligence. According to Dey [7] *"Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves."* As context-awareness deals with context reasoning to convert raw sensor data to meaningful information (situations), it can be beneficial in a large number of application domains such as medicine, emergency management, waste management, farming and agriculture, and entertainment [33]. For example, processing of raw context attribute values on the sensor/gateway may lead to a significant reduction in raw data transfer between the sensors and the applications running on clouds, as only relevant information is transferred. Context reasoning assists in reasoning about conflicting and incomplete information that is prevalent in IoT environments due to factors such as to sensor heterogeneity, data loss due to network congestion and wireless signal impairments such as signal attenuation, reflection and scattering, and manufacturing defects and variation in sensors calibration. Context reasoning may lead to the discovery of new knowledge that may be otherwise impossible when dealing with raw information by applying A.I. algorithms. Context-awareness may lead to personalization. For instance, consider a medical CPS [18] where based on the context-aware inference of user's daily activity (using data from a plethora of sensors) [35], his/her medicine dosage can be regulated by recommending which and what quantities of medicines to eat at different times of the day. Context-awareness may lead to security; for example, using context reasoning, we can determine the set of insecure sensors using metrics such as location, time, and sensor type [39]. These sensors can be disregarded when data security and privacy is of utmost concern.

Figure 2 shows a typical context-awareness cycle. First, context attribute values are sensed from the environment. Second, context reasoning is performed using the context attribute values and algorithms. Third, actuation is performed based on the reasoned context. The actuation result, as well as the corresponding sensed context, may be used to improve context reasoning if

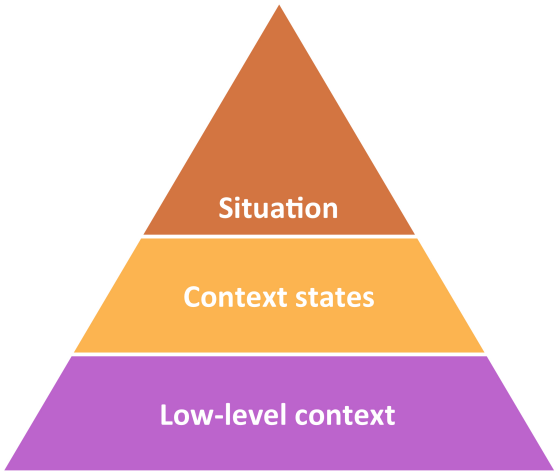

Figure 3: The context spaces model [30].

deemed necessary. For context-awareness, ICICLE considers the context spaces model (CSM) for modelling context, as shown in figure 3. The CSM motivates to *reason* about raw context attribute values collected from the sensors to determine possible *conflicting context states* about the entity (e.g., human, machine or an application process). These context states are then *fused,* i.e., some reasoning is performed to determine the overall situation of an entity. Typically in context-aware systems, reasoning can be performed using A.I.-based methods such as Fuzzy Logic, Bayesian networks and Reinforcement Learning. In ICICLE, context attribute values are collected from multiple sensors and gateways placed at homes, offices, cars, or in a factory. The raw context collected via the sensors is pre-processed on the gateway or is sent directly to the clouds running context-reasoning components. *The context-reasoning components execute algorithms to determine the situation of the cyber-physical environment and to determine actuation functions to be performed by the actuators.* For example, in a medial CPS, context collected from the sensors placed on the human body such as heart rate and insulin level is sent to the context-reasoning component to determine the situation of the patient: *"patient requires medicine"* or *"patient does not require medicine"*. This context reasoning may lead to actuation decisions: *"recommend medicine"* or *"do not recommend medicine"*. Similarly, context-aware reasoning can be applied within the Industry 4.0 paradigm or beyond to enable intelligent and efficient factories of the future.

Big data and cloud computing: The integration of IoT and CPS, will lead to data explosion and is expected to generate big data [44, 8]. Big data cannot be processed on traditional on-premise systems. Therefore, ICICLE, at its core incorporates cloud computing, which is expected to be critical for any future cyber-physical system. As mentioned in section 1, cloud computing offers highly available, scalable, reliable and cheaper access to cyber resources

(compute, storage, memory, and network). Therefore, ICICLE hosts nearly all the cyber components on the clouds such as those related to context-awareness. ICICLE may incorporate public, private or hybrid clouds depending on the application use case. For example, consider a medical CPS mentioned above, due to privacy and security requirements regarding patients data, a CPS may incorporate private clouds instead of public clouds. Major public cloud vendors such as Amazon Webservices[5], Google Compute Engine[6], and Microsoft Azure[7] provide the big data functionality. These cloud vendors offer ready-to-use, scalable and highly available big data stacks that can be used by the context reasoning components. The big data stack typically includes highly distributed file system (HDFS)[8], Apache Spark[9] or Apache Hadoop[10] as the data (context) processing frameworks. Depending on the type of CPS application domain, the context reasoning can be performed in near real-time (e.g., using Apache Spark) or in an offline mode (e.g., using Apache Hadoop).

Mobile cloud computing/edge computing/fog computing: One of the significant challenges posed by CPS is timely context gathering, storage, processing, and retrieval. Typically, context is collected from sensors and is pre-processed at the gateway nodes. The pre-processed context is then transferred to the clouds for context reasoning which can lead to some actuation in the physical world. However, the cloud data centers are centralized and distributed geographically all over the globe; the transfer of context to the clouds is expensive regarding network latency. From our tests, the average round-trip time between a gateway node placed in Skellefteå, Sweden (connected via Luleå University of Technology campus network) and Amazon cloud data center: in Stockholm, Sweden is approximately 30 ms; in Tokyo, Japan is approximately 300 ms; in Sydney, Australia data center is 400 ms, and the North California, United States data center is 200 ms. These results suggest that for mission-critical CPSs such as those related to emergency management and cognitive assistance, traditional cloud computing may not be best suited [9, 23, 25].

The areas of mobile cloud computing [25]/fog computing [38]/edge computing [36] bring cloud computing closer to IoT devices. The aim is to solve the problems regarding network latency and mobility. The premise is that instead of sending context attribute values to the centralized cloud data centers for processing, these values are processed at the first network hop itself, i.e., at the wireless access point, base station or the gateway that has a reasonable compute and storage capacity. Thereby reducing the network latency by several folds. This reduction in network latency and the augmentation of computation and storage capacity will lead to extremely powerful CPSs with near real-time decision making. These CPSs may involve human-in-the-loop (HTL) and cognitive

[5]http://aws.amazon.com [ONLINE], Access date: 5th June 2020.
[6]https://cloud.google.com/compute/ [ONLINE], Access date: 5th June 2020.
[7]https://azure.microsoft.com/en-us/ [ONLINE], Access date: 5th June 2020.
[8]https://hadoop.apache.org/docs/current1/hdfs_user_guide.html [ONLINE], Access date: 5th June 2020.
[9]https://spark.apache.org/ [ONLINE], Access date: 5th June 2020.
[10]https://hadoop.apache.org/ [ONLINE], Access date: 5th June 2020.

decision making leading to the Industry 5.0 revolution.

ICICLE supports mobile cloud computing using M^2C^2- a mobility management system for mobile cloud computing [25]. Using M^2C^2, ICICLE enables QoS-aware context processing, storage, and retrieval via edge nodes. M^2C^2 also supports multihoming and mobility management. In that, if IoT devices and gateways are mobile and are connected via several access networks such as WiFi, 4G, and Ethernet, M^2C^2 can select the best combination of network and edge/cloud. It can then handoff between the access networks and the clouds for efficient context processing and storage.

Cloud services: ICICLE is a generic framework and encompasses several ways to develop and deploy CPS services. For example, via Service Oriented Architecture (SOA) [31] or as microservices [15]. A CPS is a complex system and may include a large number of software components interacting with each other in complex ways. SOA is an already established paradigm to expose the functionality provided by ICT systems as services. SOA paradigm supports rapid, secure, on-demand, low cost, low maintenance, and standardized development, deployment, and access to software services in highly distributed environments [31], such as cloud systems. In SOA, the software services are developed and published as loosely-coupled modules. SOA services use simple object access protocol (SOAP) to communicate with each other.

Further, the services are described using Web services description language (WSDL). These services published over the Internet can be searched and discovered using Universal Description, Discovery, and Integration (UDDI), ensuring software re-use. Microservices [15] is a relatively new paradigm that defines an application as loosely-coupled services that exposes business capabilities to the outside world; here each service is developed, tested, and deployed individually without affecting each other. Thereby, microservices inherently support agile software design. Microservices communicate with each other using application programming interfaces (API). ICICLE incorporates several loosely-coupled software services. For example, the gateways and clouds run the context collection, context pre-processing service, context reasoning service for context reasoning; performance monitoring, sensor monitoring, and actuator monitoring service; actuation service; billing service; cloud monitoring service; CPS and cloud orchestration service, to name a few. These services can be deployed using SOA or microservices paradigm.

3 Case Study: ICICLE for Emergency Management

Let us consider a deep underground mine consisting of several miners extracting ore such as gold and iron. The mine runs the ICICLE-based emergency management system. The ICICLE CPS keeps track of the health of all the miners and continuously monitor their situation, such as whether they are "safe," "unsafe," or need "evacuation." The miners use controlled blasting to break away rocks

and make way for easier digging. Now consider a case that due to blasting, some rocks fall causing some miners to be trapped under them. In this scenario, ICICLE must evaluate the overall situation of the disaster area to assist the responders by providing situational knowledge about which miner needs first assistance.

Each miner wears safety-related IoT devices such as a helmet, a safety vest, and an armband. The safety vest incorporates sensors such as electrocardiogram (ECG) monitor, heart rate variability (HRV) monitor, and breathing rate monitor. The armband includes an accelerometer and a temperature gauge. These IoT devices produce a large number of context attribute values such as accelerometer, heart rate, and breathing rate values. To determine the miners' health-related situation, the IoT gateways placed throughout the mine collect these context attribute values using the context collection service. The context attribute values are produced at a very high frequency for real-time situation-awareness. Therefore, the IoT gateways pre-process these values and send them to the edge nodes present inside the mines at various locations, instead of sending them to the remote clouds for further processing.

The edge nodes and clouds run A.I.-based context reasoning services to determine miners situations. For example, based on the collected context, miner's health situation can be determined as "safe" or "unsafe" . If the situation of a miner is determined to be "unsafe" an alarm notification is triggered by ICICLE. The alarm notification, along with miner's location and health state information, is sent to the first responders that may help the miner in the shortest time possible. As emergency management requires a high degree of reliability and availability, ICICLE runs a large number of orchestration services to monitor all the edge, cloud and IoT gateway nodes. It also monitors application services such as context collection and context reasoning services at regular time intervals. Based on the monitored context, ICICLE determines the best edge, and cloud nodes to run emergency management services.

4 Future Challenges and Directions

Methodology: CPS is inter-disciplinary area encompassing advances in the disciplines such as mechanical, electrical, control and computer engineering. Each of these disciplines may have their established views on CPS; therefore the construction of CPS such as ICICLE necessitates the development of novel methodologies that brings together the best practices and advancements from all the disciplines mentioned above [34, 16, 11, 32]. We assert that there is a need to develop novel methodologies that also consider the integration of cloud computing, IoT, context-awareness and big data. Rajkumar *et al.* [34] describe steps to develop an integrated CPS. These include:

- The use of novel programming models and hardware abstractions;
- The ability to capture the limitations of the physical objects and reflect those limitations within the cyber world in the form of metrics such as

complexity, robustness, and security;

- The iterative development of system structure and models;
- Understanding the quantitative tradeoffs between cyber and physical objects based on specific constraints; and
- Enabling safety, security, and robustness considering uncertainty posed by real-world scenarios.

We believe these steps can be the starting point to extend or develop additional methodologies to realize next-generation CPS such as ICICLE.

Quality of Service and Quality of Experience: The end-to-end Quality of Service (QoS) provisioning in the cloud and IoT-enabled CPS is challenging. It is mainly due to the stochastic nature of the clouds, and the networks through data exchange are carried [24, 29]. Further, software systems may also lead to QoS variability due to their inherent architecture. Regarding networks, IoT devices may connect to the gateway using wireless access technologies such as LoRaWAN, WiFi, ZigBee, Bluetooth, and Z-wave. Each of these access network technologies is prone to signal attenuation and signal fading. Further, the data transmission from the gateway to the cloud via the ISP network, and the Internet is also prone to network congestion, delay and packet losses. Therefore, it is imperative to monitor the end to end network QoS [25]. CPS QoS also depends on clouds performance due to the multi-tenant model of the cloud systems; where via virtualization, the same underlying hardware is shared via multiple users. Multi-tenancy ensure economies of scale but may hamper applications QoS. Therefore, QoS in clouds may not be guaranteed. Application QoS can be guaranteed to a certain degree when customers are provided with dedicated hardware and networks within a cloud infrastructure, albeit at higher costs. Software systems may also hamper the overall QoS due to due to limitations of software libraries and systems that may not be able to avail hardware performance, this can be due to higher developmental costs of the software systems, or may be due to improper software design for a particular application scenario. Therefore, cloud-integrated CPS requires holistic monitoring across cloud and network stack along with physical devices.

We argue that the success of next-generation CPS hinges on the understanding end-users perception of quality regarding an application or service, or users quality of experience (QoE) [10]. QoE is often misunderstood and is narrowly associated with QoS metrics [26]. QoE is users' perception of underlying QoS along with a person's preferences towards a particular object or a service. It depends on person's attributes related to his/her expectations, cognitive abilities, behaviour, experiences, object's characteristics (e.g., mobile device screen size, and weight) and the environment [26]. Till date, QoE metrics have been mainly investigated from communication networks, multimedia (such as voice and media streaming) and gaming perspectives. However, QoE metrics have not been studied extensively in the context of cloud computing and especially from IoT perspective which are highly dynamic, stochastic and sophisticated

systems [22]. There is a need to develop novel QoE models that consider the entire cloud and IoT ecosystem on which next-generation CPS will be based. For instance, in the mining disaster use case mentioned above, QoE provisioning for the responder is critical from him/her to save the lives of the evacuee. CPS like ICICLE should not only aim to maximize QoS, but also aim to adapt the content, minimize service disruptions and in the worst-case scenario, provide graceful degradation of service such that the responders are *satisfied* with the CPS and *accept* it for future use.

Service level agreement (SLA): Ensuring the SLAs in future CPS is challenging as it involves clouds as well as the IoT. SLA in clouds has been studied quite extensively [17]. These studies span across all the cloud layers namely Infrastructure-as-a-Service, Platform-as-a-Service, and Software-as-a-Service and cover numerous metrics related to performance, cost, security and privacy, governance, sustainability, and energy efficiency. However, in reality, each cloud vendor offers their own SLAs to their customers and are usually limited to availability/uptime metric. Further, there is a lack of a unified SLA framework across cloud providers that hinders cloud adoption. Regarding IoT applications and services, metrics such as availability, reliability, scalability, throughput, access time and delay, usability, level of confidentiality have been studied [1].

To the best of our knowledge, in the context of cloud and IoT integrated CPS, no standardized SLA framework exists. SLA definition, monitoring, and adherence in CPS can, therefore, be very challenging. Firstly, due to the presence of a large number of parameters mentioned above and secondly, determining the right combination of parameters in an IoT application domain can be an exhaustive task. Cloud-based IoT services can be very complicated as they involve the interconnection of devices to the clouds; and IoT service provisioning to the end-users via the Internet. Therefore, each of this step may have different SLAs in place. For instance, stakeholders offering sensor deployment, the Internet service providers (ISP), the cloud providers, and the application/service providers may each offer different SLAs. Therefore, determining a right SLA that combines multiple SLAs for end-to-end IoT service provisioning remains a longer-term and a challenging goal [1].

Trust, privacy and security: Trust, privacy and security: are essential considerations for a CPS [16]. As discussed above, a CPS consists of several components (see figure 1) such as sensors, actuators, servers, network switches, and routers, and myriad applications. Complex interdependencies may exist between these components; therefore, security-related failure in one component may propagate to another component. For example, a denial of service attack that mimics a large number of sensors towards a context collection service may render it unusable and may not only lead to interruptions in context reasoning but may cause a complete halt of the CPS. One can consider this as the worst-case scenario for any mission-critical CPSs such as the emergency management CPS mentioned in the previous section. Khaitan and McCalley [16] also note that installing new software patches to several application components is challenging due to the time-critical nature of the CPS. CPSs are also prone to

man-in-the-middle attacks as well as the attacks on physical infrastructure, for example, smart meters as part of the smart grid CPS can be a target of not only vandalism but also as part of the targeted cyber attack. We assert that a holistic approach considering trust, privacy, and security-related challenges should be considered when building a CPS. In particular, these challenges should be considered in an end-to-end manner, i.e., starting from the physical devices to the end-user (humans/machines) and should then be formally verified and tested using state-of-the-art benchmarks and tools.

Mobility: poses a significant challenge for future CPSs. The users and devices such as sensors placed on vehicles, smartphones, tablets are expected to be mobile. For example, consider a healthcare CPS that determines users health in near real-time and alerts them and their doctors is something extraordinary occurs regarding their health. The users wear products such as Hexoskin [11] to that measure physiological parameters such as breathing rate, heart rate, acceleration, cadence, heart rate, and ECG. As the users are typically mobile, for example, they go to their workplace, gym, use public transport, their Hexoskin monitors their vital parameters and send the parameter values to their smartphones; the smartphones then transfer these parameter values via 4G or WiFi networks to the clouds for processing. The processed data is then either send back to users smartphones or is sent to their doctors. As the users carrying their smartphones are mobile, their smartphones may connect to several wireless access networks such as WiFi and 4G. These access networks exhibit stochastic performance characteristics due to issues like signal attenuation, and reflection; users smartphones may handoff between several access technologies leading to disconnection [25].

Further clouds may also exhibit stochastic performance characteristics due to unpredictable workloads and multi-tenancy [19, 24]. Lastly, network link between the smartphones and the clouds may be congested or maybe far away (regarding round-trip times) [25] leading to additional transmission delays. All these factors necessitate efficient mobility management to ensure performance guarantees [25, 40], One way to deal with the mobility issue is to consider computation and storage offloading to the edge nodes in conjunction network mobility management [25]. However, further complications arise regarding data management, trust, and privacy. Therefore, there is a need to develop novel CPS-aware mobility management protocols that inherently support QoS, trust, privacy, and security.

Middleware Platforms: may assist in the integration of IoT, clouds, and CPS by providing standardized interfaces for data collection, storage, and retrieval. Standardized interfaces are essential to deal with heterogeneity in device types, application and network protocols, software stacks, vendor-specific APIs, and data models for data representation. Cloud-based IoT middleware platforms may prove to be crucial to integrate cloud systems and IoT to realize next-generation CPS by solving at least some of the requirements presented above. In excess of 500 IoT middleware systems exists that integrate IoT de-

[11] https://www.hexoskin.com/ [ONLINE]. Access date: 1st June 2020.

vices with clouds [28]. For example, some of the IoT middleware include Xively [12], AWS IoT[13], Microsoft Azure IoT HuB[14], ThingsBoard[15], FIWARE[16], OpenIoT[17], and Kaa[18]. It is imperative that IoT middlewares are highly scalable, reliable, and available and should cater to a large of the application use cases such as those related to smart cities [8, 2]. To the best of our knowledge, there is a dearth of research that comprehensively benchmarks the aforementioned IoT middlewares and presents a selection of them that can be used readily by either industry and academia. Recently Araujo *et al.* [2], have presented results regarding IoT platform benchmarking. However more work is required to build future cloud-based IoT middleware for CPS.

Context-awareness: is the key to creating value out of the big data originating from the IoT devices in a CPS. As mentioned above, context reasoning will enable intelligence in CPSs by dealing with raw, conflicting, and incomplete context values. Therefore, novel context reasoning algorithms and frameworks are required to be integrated with IoT middlewares for intelligent decision making. In the past two decades, significant advances have been made in area of context-aware computing. For instance, seminal work done in this area [7, 30, 12, 43], can be leveraged to build intelligent context-aware CPSs. We believe their work should be combined with recent advances in big data, artificial intelligence, and cloud computing to harness their true potential [44, 8]. IoT brings it own set of challenges due to their expected massive scale deployments. These challenges include context-aware sensor/actuator/service representation, discovery and selection [33]. Recent work [20] deals with these challenges. However, their integration with IoT middlewares and their rigorous testing regarding scalability and performance is still warranted.

5 Conclusion

Integration of areas such as cloud computing, IoT, and big data is crucial for developing next-generation CPSs. These CPSs will be a part of future smart cities and are expected to enhance areas like agriculture, transportation, manufacturing, logistics, emergency management, and waste management. However, building such a CPS is particularly challenging due to a large number of issues in integrating the above-mentioned areas. This chapter discussed in details several such challenges regarding context-awareness, quality of service and quality of experience, mobility management, middleware platforms, service level agreements, trust, and privacy. This chapter also proposes and develops ICICLE: A

[12]https://xively.com/ [ONLINE], Access date: 9th July 2020.
[13]https://aws.amazon.com/iot/ [ONLINE], Access date: 9th July 2020.
[14]https://azure.microsoft.com/en-us/services/iot-hub/ [ONLINE], Access date: 9th July 2020.
[15]https://thingsboard.io/ [ONLINE], Access date: 9th July 2020.
[16]https://www.fiware.org/ [ONLINE], Access date: 9th July 2020.
[17]http://www.openiot.eu/ [ONLINE], Access date: 9th July 2020.
[18]https://www.kaaproject.org/ [ONLINE], Access date: 9th July 2020.

Context-aware IoT-based Cyber-Physical System that integrates cloud computing, IoT, and big data to realize next-generation CPSs.

Acknowledgement

The research is conducted under the SSiO project which is supported by the EU Regional Development Fund (Tillväxtverket). More information regarding the SSiO project can be found on this website: https://ssio.se/.

References

[1] A. Alqahtani, Y. Li, P. Patel, E. Solaiman, and R. Ranjan. End-to-end service level agreement specification for iot applications. In *2018 International Conference on High Performance Computing Simulation (HPCS)*, pages 926–935, July 2018.

[2] V. Araujo, K. Mitra, S. Saguna, and C. Åhlund. Performance evaluation of fiware: A cloud-based iot platform for smart cities. *Journal of Parallel and Distributed Computing*, 132:250 – 261, 2019.

[3] A. Bahga and Madisetti V. *Cloud Computing: A Hands-on Approach*. CreateSpace Independent Publishing Platform, 2014.

[4] A. Bahga and Madisetti V. *Internet of Things: A Hands-on Approach*. VPT, 2014.

[5] G. C. Christos. Smart cities as cyber-physical social systems. *Engineering*, 2(2):156 – 158, 2016.

[6] P. Derler, E. A. Lee, and A. S. Vincentelli. Modeling cyber physical physical systems. *Proceedings of the IEEE*, 100(1):13–28, Jan 2012.

[7] A.K. Dey and G.D. Abowd. Toward a better understanding of context and context-awareness, gvu technical report git-gvu-99-22, college of computing, georgia institute of technology. ftp://ftp.cc.gatech.edu/pub/gvu/tr/1999/99-22.pdf.

[8] M. Días, C. Martín, and B. Rubio. State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing. *Journal of Network and Computer Applications*, 67:99 – 117, 2016.

[9] K. Ha, Z. Chen, W. Hu, W. Richter, P. Pillai, and M. Satyanarayanan. Towards wearable cognitive assistance. Technical Report CMU-CS-13-34, Carnegie Mellon University, December 2013.

[10] F. Hammer, S. Egger-Lampl, and S. Möller. Position paper: Quality-of-experience of cyber-physical system applications. In *2017 Ninth International Conference on Quality of Multimedia Experience (QoMEX)*, pages 1–3, 2017.

[11] P. Hehenberger, B. Vogel-Heuser, D. Bradley, B. Eynard, T. Tomiyama, and S. Achiche. Design, modelling, simulation and integration of cyber physical systems: Methods and applications. *Computers in Industry*, 82:273 – 289, 2016.

[12] K. Henricksen and J. Indulska. Developing context-aware pervasive computing applications: Models and approach. *Pervasive and Mobile Computing*, 2(1):37 – 64, 2006.

[13] G. Jayavardhana, B. Rajkumar, M. Slaven, and P. Marimuthu. Internet of things (iot): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7):1645 – 1660, 2013. Including Special sections: Cyber-enabled Distributed Computing for Ubiquitous Cloud and Network Services & Cloud Computing and Scientific Applications - Big Data, Scalable Analytics, and Beyond.

[14] Ngo . K., S. Saguna, K. Mitra, and C. Åhlund. Irehmo: An efficient iot-based remote health monitoring system for smart regions. In *2015 17th International Conference on E-health Networking, Application Services (HealthCom)*, pages 563–568, Oct 2015.

[15] A. Karmel, R. Chandramouli, and M. Iorga. Nist definition of microservices, application containers and system virtual machines. Technical report, National Institute of Standards and Technology, 2016.

[16] S. K. Khaitan and J. D. McCalley. Design techniques and applications of cyberphysical systems: A survey. *IEEE Systems Journal*, 9(2):350–365, June 2015.

[17] S.R. Khan and L. B. Gouveia. Cloud computing service level agreement issues and challenges: A bibliographic review. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 7(3):209—229, 2018.

[18] I. Lee and O. Sokolsky. Medical cyber physical systems. In *Design Automation Conference*, pages 743–748, June 2010.

[19] P. Leitner and J. Cito. Patterns in the chaos—a study of performance variation and predictability in public iaas clouds. *ACM Trans. Internet Technol.*, 16(3):15:1–15:23, April 2016.

[20] A. Medvedev, A. Hassani, P. D. Haghighi, S. Ling, M. Indrawan-Santiago, A. Zaslavsky, U. Fastenrath, F. Mayer, P. P. Jayaraman, and N. Kolbe. Situation modelling, representation, and querying in context-as-a-service iot platform. In *2018 Global Internet of Things Summit (GIoTS)*, pages 1–6, June 2018.

[21] P. Mell and T. Grance. The nist definition of cloud computing: Recomendations of the national institute of standards and technology. *National Institute of Standards and Technology*, (800-145):7, Septmeber 2011.

[22] D. Minovski, C. Åhlund, and K. Mitra. Modeling quality of iot experience in autonomous vehicles. *IEEE Internet of Things Journal*, 7(5):3833–3849, 2020.

[23] K. Mitra, Saguna, and C. Ahlund. A mobile cloud computing system for emergency management. *Cloud Computing, IEEE*, 1(4):30–38, Nov 2014.

[24] K. Mitra, S. Saguna, C. Åhlund, and R. Ranjan. Alpine: A bayesian system for cloud performance diagnosis and prediction. In *2017 IEEE International Conference on Services Computing (SCC)*, pages 281–288, June 2017.

[25] K. Mitra, S. Saguna, C. Ahlund, and D. Granlund. M^2c^2: A mobility management system for mobile cloud computing. In *Wireless Communications and Networking Conference (WCNC), 2015 IEEE*, pages 1608–1613, March 2015.

[26] K. Mitra, A. Zaslavsky, and C. Åhlund. Context-aware qoe modelling, measurement, and prediction in mobile computing systems. *IEEE Transactions on Mobile Computing*, 14(5):920–936, 2015.

[27] L. Monostori, B. Kádár, T. Bauernhansl, S. Kondoh, S. Kumara, G. Reinhart, O. Sauer, G. Schuh, W. Sihn, and K. Ueda. Cyber-physical systems in manufacturing. *CIRP Annals*, 65(2):621 – 641, 2016.

[28] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng. Iot middleware: A survey on issues and enabling technologies. *IEEE Internet of Things Journal*, 4(1):1–20, Feb 2017.

[29] A. Noor, K. Mitra, E. Solaiman, A. Souza, D. N. Jha, U. Demirbaga, P.P. Jayaraman, N. Cacho, and R. Ranjn. Cyber-physical application monitoring across multiple clouds. *Computers & Electrical Engineering*, 77:314 – 324, 2019.

[30] A. Padovitz, S. W. Loke, and A. Zaslavsky. Towards a theory of context spaces. In *Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on*, pages 38–42.

[31] M. P. Papazoglou and D. Georgakopoulos. Introduction: Service-oriented computing. *Commun. ACM*, 46(10):24–28, October 2003.

[32] L. Paulo, W. C. Armando, and K. Stamatis. Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges. *Computers in Industry*, 81:11 – 25, 2016. Emerging ICT concepts for smart, safe and sustainable industrial systems.

[33] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos. Context aware computing for the internet of things: A survey. *IEEE Communications Surveys Tutorials*, 16(1):414–454, First 2014.

[34] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic. Cyber-physical systems: The next computing revolution. In *Design Automation Conference*, pages 731–736, June 2010.

[35] S. Saguna, A. Zaslavsky, and D. Chakraborty. Complex activity recognition using context-driven activity theory and activity signatures. *ACM Trans. Comput.-Hum. Interact.*, 20(6):32:1–32:34, December 2013.

[36] M. Satyanarayanan, G. Lewis, E. Morris, S. Simanta, J. Boleng, and Kiryong Ha. The role of cloudlets in hostile environments. *Pervasive Computing, IEEE*, 12(4):40–49, Oct 2013.

[37] E. Simmon, K. Kim, E. Subrahmanian, R. Lee, F. Vaulx, Y. Murakami, K. Zettsu, and D. R. Sriram. A vision of cyber-physical cloud computing for smart networked systems. Technical report, National Institution of Standands and Technology, 2013.

[38] L. M. Vaquero and L. Rodero-Merino. Finding your way in the fog: Towards a comprehensive definition of fog computing. *SIGCOMM Comput. Commun. Rev.*, 44(5):27–32, October 2014.

[39] K. Wan and V. Alagar. Context-aware security solutions for cyber-physical systems. *Mobile Networks and Applications*, 19(2):212–226, Apr 2014.

[40] J. Warley, F. Adriano, D. Kelvin, and N. de S. Jose. Supporting mobility-aware computational offloading in mobile cloud environment. *Journal of Network and Computer Applications*, 94:93 – 108, 2017.

[41] Y. Xuejun, C. Hu, Y. Hehua, Z. Caifeng, and Z. Keliang. Cloud-assisted industrial cyber-physical systems: An insight. *Microprocessors and Microsystems*, 39(8):1262 – 1270, 2015.

[42] X. Yao, J. Zhou, Y. Lin, Y. Li, H. Yu, and Y. Liu. Smart manufacturing based on cyber-physical systems and beyond. *Journal of Intelligent Manufacturing*, pages 1–13, Dec 2017.

[43] J. Ye, S. Dobson, and S. McKeever. Situation identification techniques in pervasive computing: A review. *Pervasive and Mobile Computing*, 8(1):36 – 66, 2012.

[44] A. Zaslavsky, C. Perera, and D. Georgakopoulos. Sensing as a service and big data. In *International Conference on Advances in Cloud Computing (ACC)*, pages 21–29, 2012.