Cloud Computing System Analysis for ŠKODA AUTO

Analýza cloud computing systémů pro ŠKODA AUTO

Project Report

Marek Rychlý and Dušan Kolář

The Project Ordered by

Brand Planning, Production and Logistics, ŠKODA AUTO a.s.

Brno University of Technology, Faculty of Information Technology

Contents

1 Introduction to Cloud Computing

Cloud computing can be defined as a new style of computing in which dynamically scalable and often virtualised resources are provided as a services over the Internet. Cloud computing has become a significant technology trend, and many experts expect that cloud computing will reshape information technology (IT) processes and the IT marketplace. With the cloud computing technology, users use a variety of devices, including PCs, laptops, and smartphones to access programs, storage, and application-development platforms over the Internet, via services offered by cloud computing providers. Advantages of the cloud computing technology include cost savings, high availability, and easy-to-use scalability. [1]

Over the past years, there has been increasing need for a ubiquitous provision of computing resources. Historically, from a technological perspective, cloud computing started to evolve from mainframe architectures where large mainframe computers provided computation and storage services centrally at dedicated data-centres, through more distributed and decentralized client-server architectures where specialized servers provided their services via Internet, to personal computers that eventually become ubiquitous, small personal devices. All these architectures made sense for particular use-cases and in their time, however, they suffered from many problems limiting their availability and possible applications. The problems include the following:

- high maintenance/infrastructure costs – It was difficult to maintain hardware (HW) and software (SW) of the mainframes or the servers and their client applications to keep required quality of service according to service level agreements. For example, high availability of critical services required expensive solutions such as redundant systems, hot backups, spare preconfigured components, minimal or no downtime (even for the maintenance), etc.

- low scalability/agility – User requirements and utilisation of HW and SW systems typically change over time with emerging business needs. Ability to upscale the systems with increasing requirements to keep the quality of service (such as response time per request) or to downscale the systems to save utilised resources and reduce costs is quite difficult and may not be economically or physically possible to do on short notice and/or repeatedly.

- problematic out-sourcing – The out-sourcing of IT is quite common, not only for the small and middle enterprises. However, in the case of existing HW and SW solutions located in particular data centres, built on particular platform provided by a particular vendor, or distributed and maintained in particular way, it may be difficult to isolate these solutions and make them ready for their out-sourcing. Even in the case of already outsourced IT solutions, it is usually quite expensive to move them to different provider.

- unclear accounting – IT departments are usually considered as cost centres provided with a fixed annual budget for operating its infrastructure and providing services to other departments. While the other departments consume the IT services to perform

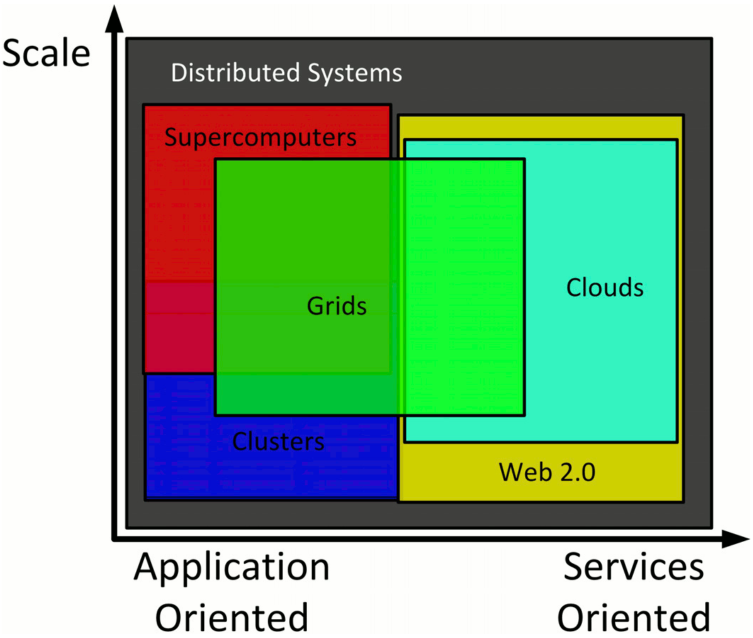


Figure 1.1: Grids and clouds overview (adopted from [2]).

> their business and generate a profit, it is difficult to map the utilisation of IT resources through IT services to the organization profit and to prove that the IT resources are providing value for the money that was spent.

These problems and others were addressed by various means, even before the era of cloud computing. There were invested many efforts to distributed computing (that result into Open MPI standard[1]), virtualisation (well-established closed- and open-source solutions), virtual private networks (VPNs) (to connect local branches of organisations and make their IT services available globally), etc. For example, grid computing, one of these historical approaches proving that the cloud computing is not a completely new concept, tried to reduce the cost of computing and increase reliability and flexibility by transforming computers from something that we buy and operate ourselves to something that is operated by a third party [2]. However, grid computing, cloud computing, as well as other similar approaches differ in the scale and the focus as depicted in Figure 1.1. Moreover, all these solutions require fast networking to be applied globally and since the Internet only started to offer significant bandwidth in the nineties and later, cloud computing has not become trend and widely adopted until the last 10 years.

1.1 Cloud Computing Terms

In 2011, National Institute of Standards and Technology (NIST) of United State Department of Commerce published a definition of cloud computing [3] to characterize its important aspects, to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. According to NIST [3], 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

[1] `https://www.open-mpi.org/`

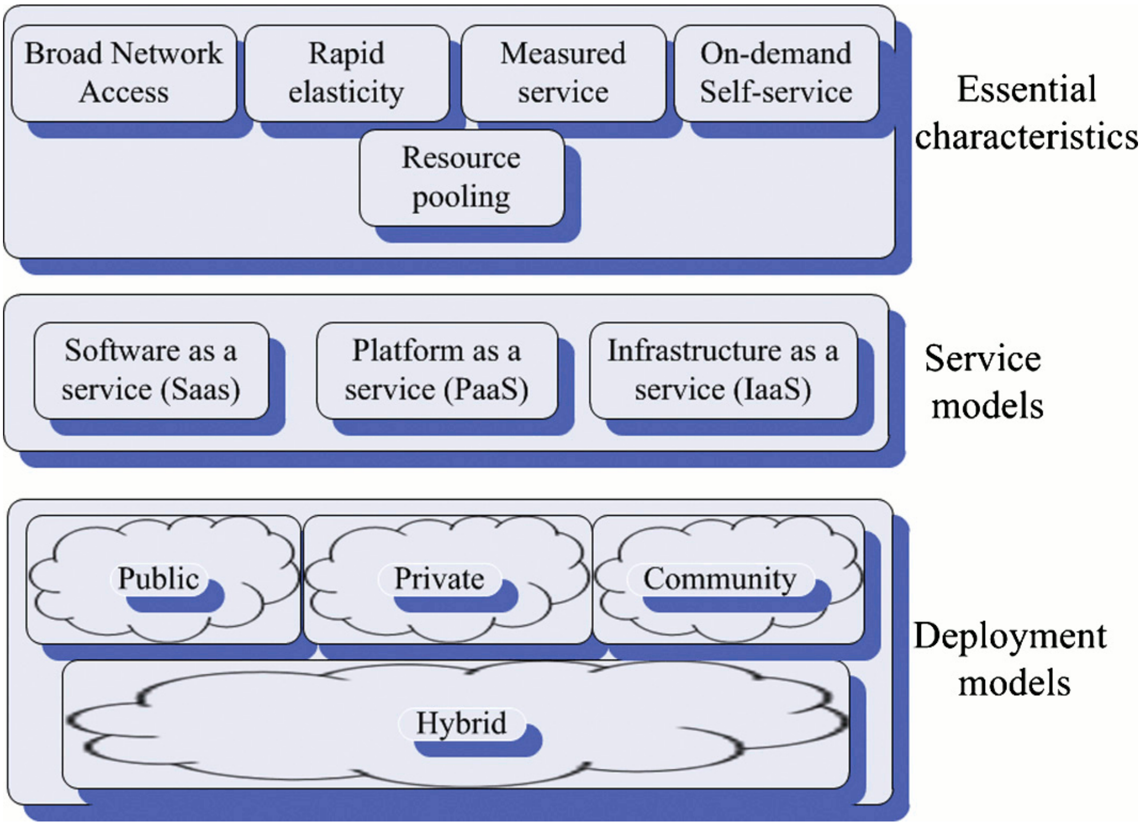


Figure 1.2: NIST definition of cloud computing (adopted from [4]).

be rapidly provisioned and released with minimal management effort or service provider interaction.

As depicted in Figure 1.2, the cloud model is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured service), three service models (Infrastructure as a Service, Platform as a Service, Software as a Service), and four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud). In the following section, the essential characteristics, the service models, and the deployment models will be described and discussed to establish cloud computing terms for this document.

1.1.1 Essential Characteristics

The NIST definition of cloud computing [3] lists the following five essential characteristics:

- *On-demand self-service* – A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

- *Broad network access* – Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

- *Resource pooling* – The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data-centre). Examples of resources include storage, processing, memory, and network bandwidth.

- *Rapid elasticity* – Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurately with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

- *Measured service* – Cloud systems automatically control and optimize resource use by leveraging a metering capability[2] at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, verified, and reported, providing transparency for both the provider and consumer of the utilised service.

From a technological point of view, there is yet another characteristic of cloud computing – multi-tenancy. It is not the essential characteristic according to NIST, however, the multi-tenancy is quite necessary to ensure required quality of service and provide basic security in cloud. Cloud Security Alliance define the multi-tenancy as follows [5]:

- *Multi-tenancy* – In its simplest form, multi-tenancy implies use of same resources or application by multiple consumers that may belong to same organization or different organization. The impact of multi-tenancy is visibility of residual data or trace of operations by other user or tenant. Multi-tenancy in cloud service models implies a need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies.

1.1.2 Service Models

By NIST [3], the cloud computing can be categorized according to provided service to the following:

- *Software as a Service (SaaS)* – The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure[3]. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

- *Platform as a Service (PaaS)* – The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider[4].

[2] Typically this is done on a pay-per-use or charge-per-use basis.

[3] A cloud infrastructure is the collection of HW and SW that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the HW resources that are necessary to support the cloud services being provided and typically includes server, storage, and network components. The abstraction layer consists of the SW deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

[4] This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.

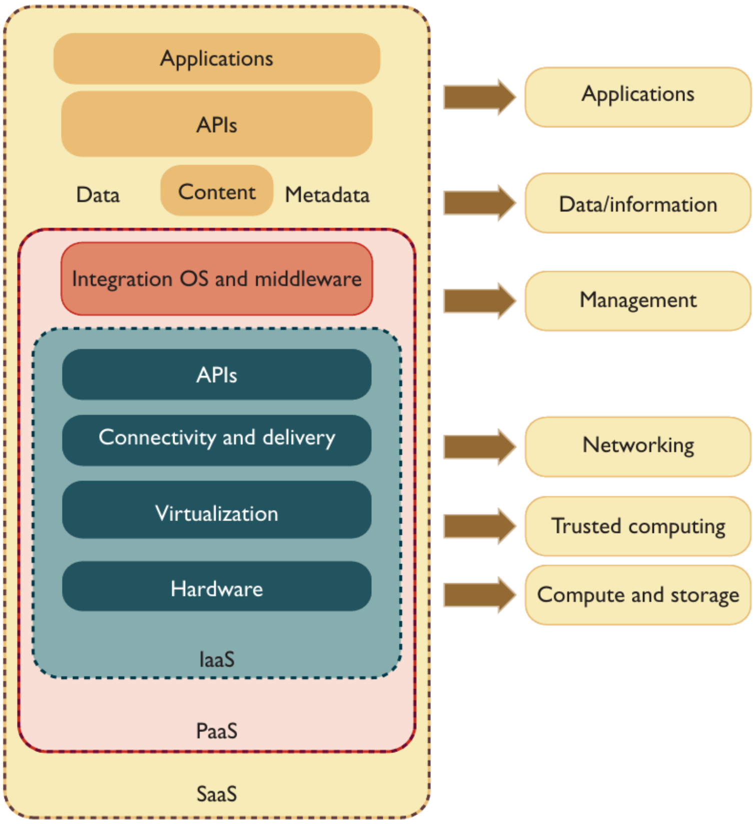


Figure 1.3: Three cloud service models with provided services (adopted from [6]).

The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

- *Infrastructure as a Service (IaaS)* – The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary SW, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of selected networking components (e.g., host firewalls).

The cloud service models encapsulate and publish various services (see Figure 1.3) in a HW/SW stack, from low-level services to access provided HW and infrastructure resources (native or virtualised) for system and network administrators in the case of IaaS; through operating system services, SW components and middleware for developers in the case of PaaS; to ready-to-use applications and high-level application programming interfaces (APIs) for end-users in the case of SaaS. In this layered stack of service models, each service model inherits the capabilities of the service model below.

Besides the three service models above, that are known together as the SPI model (SPI), there are many other models described in the literature, such as Network as a Service (NaaS), Storage as a Service (StaaS), or Identity as a Service (IdaaS).

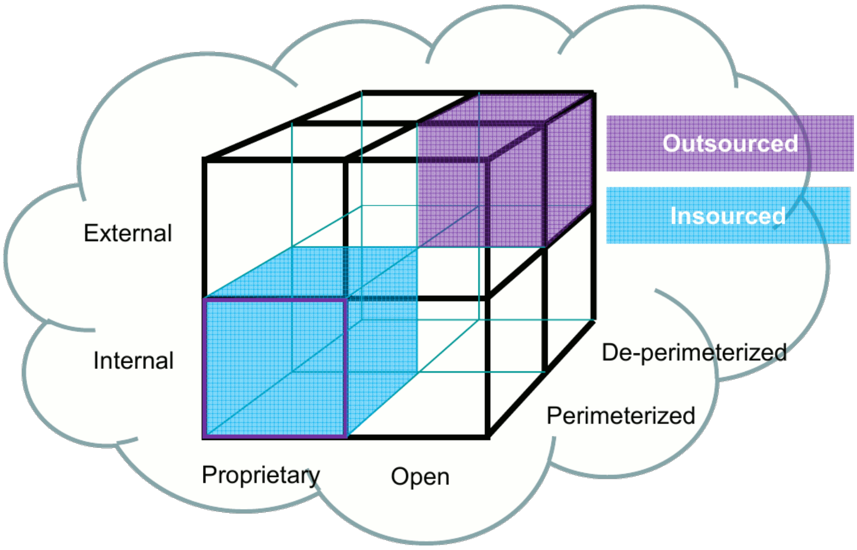


Figure 1.4: The Jericho Forum Cloud Cube Model (adopted from [7]).

1.1.3 Deployment Models

NIST described four deployment models for cloud computing [3] dealing with possible locations of the cloud:

- *Private cloud* – The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

- *Community cloud* – The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

- *Public cloud* – The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

- *Hybrid cloud* – The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

1.1.4 Cloud Cube Model (CCM)

In 2009, the Jericho Forum [7] identified four criteria to differentiate cloud formations from each other and the manner of their provision. The Cloud Cube Model (CCM) is depicted in Figure 1.4 and it summarizes these four dimensions as follows [7]:

- *Internal (I) / External (E) dimension* defines the physical location of the data in the cloud, if it exists inside or outside the organization's physical boundaries, respectively.

An example of the internal cloud would be a shared storage with virtualised hard disks in an organization's data centre, while the same storage in Amazon SC3 would be an example of the external cloud.

- *Proprietary (P) / Open (O) dimension* defines the state of ownership of the cloud technology, services, interfaces, etc. Proprietary means that a service provider is keeping the means of provision under its ownership, while open means that there are likely to be more suppliers of a non-proprietary technology. In the case of open cloud, a customer will not be constrained in its ability to share data or applications and collaborate with selected parties using the same open technology. Therefore, the P/O dimension indicates the degree of interoperability, as well as enabling "data/application transportability" between the current systems and other cloud forms, and the ability to withdraw data from a cloud or to move it to another cloud without constraints.

- *Perimeterised (Per) / De-perimeterised (D-p) Architectures dimension* represents the "architectural mindset" of the cloud solution where cloud access points are running inside or outside of an IT infrastructure perimeter of a customer organisation, respectively.

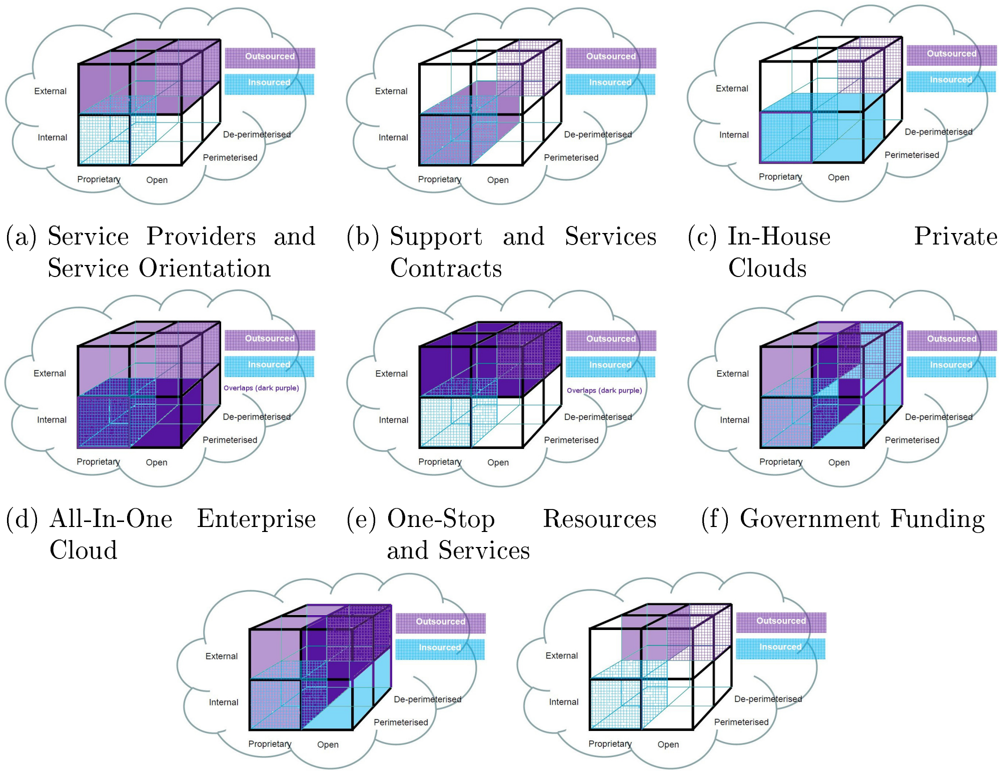
  The perimeterised cloud architecture implies continuing to operate within the traditional IT perimeter. This is often signalled by "network firewalls" that control the access to cloud services in the same way as in the case of non-cloud services running inside a traditional, though virtual, perimeter of the organisation. In this case, the organization's perimeter is often simply extended into the external cloud computing domain using a VPN or a virtual server operating in the organisation's Internet Protocol (IP) domain, making use of its directory services to control access.

  De-perimeterised cloud architecture assumes that the system perimeter is managed by a cloud provider and the cloud services must be explicitly protected, which is much more difficult (e.g., data would be encapsulated with meta-data and mechanisms that would protect the data from inappropriate usage must exist). For example, an early experience of using the external proprietary cloud form represented by Amazon SC3 has involved a combination of perimeterised Amazon virtual servers and de-perimeterised public data sets to create private results that are then repatriated to the internal non-cloud environment.

- *Insourced / Outsourced dimension* describes who is managing delivery of the cloud services utilised by an organisation. The services can be provided by the organisation's staff under its full control, or by a contracted third party. This is primarily a policy issue (i.e., a business decision, not a technical or architectural decision) which must be embodied in a contract with the cloud provider. In the CCM diagram, this fourth dimension is shown by two colours; any of the eight cloud forms (Per IP, IO, EP, EO; and D-p IP, IO, EP, EO) can take either colour.

The CCM illustrates permutations of values in the dimensions above that are available in cloud offerings today. The model presents possible values in the four criteria/dimensions in order to differentiate cloud "formations" and the manner of their provision, and to understand how cloud computing affects the way in which security might be approached [5]. The security aspect of the cloud computing will be further discussed in Section 2.3.

The CCM is also utilised by [8] to review current cloud computing business models and to present proposals on how organisations can achieve sustainability by adopting one of the eight cloud computing business models with their known strengths and weaknesses (see Figure 1.5):



(a) Service Providers and Service Orientation

(b) Support and Services Contracts

(c) In-House Private Clouds

(d) All-In-One Enterprise Cloud

(e) One-Stop Resources and Services

(f) Government Funding

(g) Venture Capitals

(h) Entertainment and Social Networking

Figure 1.5: Cloud computing business models (adopted from [8]).

- *Service Provider and Service Orientation* – for external outsourced clouds providing either of IaaS, PaaS, or SaaS solutions,

- *Support and Services Contracts* – for internal outsourced proprietary clouds covering either of IaaS, PaaS, or SaaS services,

- *In-House Private Clouds* – for internal insourced perimeterised clouds implementing the SaaS model,

- *All-In-One Enterprise Cloud* – for internal insourced perimeterised clouds combined with completely outsourced cloud solutions to cover all service models,

- *One-Stop Resources and Services* – for external cloud solutions where both insourcing and outsourcing is necessary, usually in the case of community clouds,

- *Government Funding* – for governmentally funded organisations utilising outsourced proprietary clouds in private sector or insourced open cloud solutions in the case of academic institutions,

- *Venture Capitals* – for private companies, usually start-ups, that utilise outsourced proprietary clouds, external outsourced open clouds, or insourced open cloud solutions,

- *Entertainment and Social Networking* – for external outsourced de-perimeterised proprietary clouds implementing SaaS service models.

The cloud computing business model above will be utilised in the comparison of available cloud services in Chapter 3.

1.2 State of the Art of Cloud Computing and Future Trends

As stated in [1], cloud computing is a distributed computing paradigm that mixes aspects of grid computing (“...HW and SW infrastructure that provides dependable, consistent, pervasive, and inexpensive access to high-end computational capabilities” [9]), Internet Computing (“...a computing platform geographically distributed across the Internet” [10]), Utility computing (“a collection of technologies and business practices that enables computing to be delivered seamlessly and reliably across multiple computers, ...available as needed and billed according to usage, much like water and electricity are today” [11]), Autonomic computing (“computing systems that can manage themselves given high-level objectives from administrators” [12]), Edge computing (“...provides a generic template facility for any type of application to spread its execution across a dedicated grid, balancing the load ...” [13]) and Green computing (from the assumption that energy costs of IT are related to the environmental pollution [1]).

Because of these aspects of the cloud computing and tight bonds between cloud computing and many other research fields and technologies, emerging topics of interests and innovations in the related fields necessarily affect also the direction of cloud computing research. In the following sections, two of the state-of-the-art approaches to cloud computing in manufacturing industry will be described and possible future trends will be outlined.

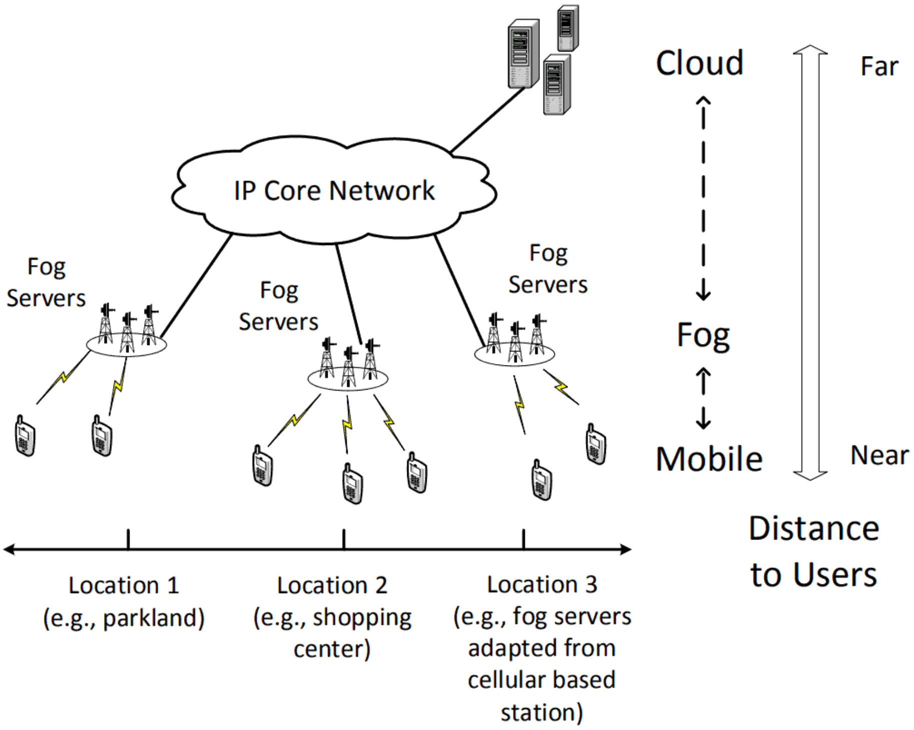

IP Core Network
Fog Servers
Fog Servers
Fog Servers
Cloud
Fog
Mobile
Far
Near
Distance to Users
Location 1 (e.g., parkland)
Location 2 (e.g., shopping center)
Location 3 (e.g., fog servers adapted from cellular based station)

Figure 1.6: Fog computing architecture (adopted from [14]).

1.2.1 Edge Computing and Fog Computing

Our networking today is shaped by two obvious trends [14]:

- *Cloud-based Internet* – Cloud computing has already evolved as the key computing infrastructure for Internet with full-fledged services encompassing not only contents but also communications, applications, and commerce. As reported, around 90% of global Internet users are now relying on the services provided by cloud, either directly through consumer services or indirectly through their service provider's reliance upon different commercial clouds.

- *Proliferation of mobile (edge) computing* – Since 2011, the smartphone shipment worldwide has overtook that of PCs. To date, the smartphone penetration in U.S. has reached 80%. As predicted by Cisco, the average connected devices per person will reach 6.58 in 2020. With various smart devices with strong computing and communication power, a variety of mobile computing applications, e.g., virtual reality, sensing, and navigation, have emerged and resulted in the fundamental changes in the pattern that people live.

Fog computing is trying to merge the two trends above. Cloud services are moved closer to their consumers by establishing network and mobile computing devices participating in the cloud at the edge of network as providers of the individual cloud services (see Figure 1.6), while the core cloud computing technology provides shared services to support the devices in accordance with objectives of the edge-centric computing [15]. In fog computing [16], services can be hosted at end devices such as set-top-boxes or access points. The infrastructure of this new distributed computing allows applications to run as close as possible to sensed actionable and massive data, coming out of people, processes, and things. Such fog computing concept, actually a cloud computing close to the “ground”, creates automated response that drives the value.

Fog computing was recently defined in [17] as a scenario where a huge number of heterogeneous (wireless and sometimes autonomous) ubiquitous and decentralised devices communicate and potentially cooperate among them and with the network to perform storage and processing tasks without the intervention of third parties. These tasks can be for supporting basic network functions or new services and applications that run in a sandboxed environment. Users leasing part of their devices to host these services get incentives for doing so.

As fog computing is implemented at the edge of the network, it provides low latency, location awareness and improves quality of service (QoS) for streaming and real time applications. Moreover, this new infrastructure supports heterogeneity as fog devices include end-user devices, access points, edge routers and switches. The fog paradigm is well positioned for real time Big data analytics, supports densely distributed data collection points and provides advantages in entertainment, advertising, personal computing and other applications. [16]

Examples of Fog Computing

Typical examples of fog computing applications include industrial automation, transportation, and networks of sensors and actuators [16]. In these use-cases, fog computing and cloud computing coexist in a symbiotic relationship. While local fog computing nodes in factories, cars or smart-cities provide localization, therefore enabling low latency and context awareness mentioned above, the cloud computing provides necessary global centralization [18].

In the first example of industrial automation, fog computing can be used in Industry 4.0 factories where it can effectively separate manufacture data in the nearest level in order to save the speed of calculation, bandwidth, efficiency and support decentralization, so that only useful data will be provided to control, analysis, and management levels [19].

In the second example, fog computing in transportation represents an ideal platform to deliver a rich menu of services in infotainment, safety, traffic support, and analytics, as it has a number of suitable attributes: geo-distribution (throughout cities and along roads), mobility and location awareness, low latency, heterogeneity, and support for real-time interactions such as in the case of a smart traffic light system in a smart city[5] [18].

Finally, the third example utilises fog computing in a smart grid where fog collectors at the edge ingest the data generated by grid sensors and devices. Some of this data relates to protection and control loops that require real-time processing (from milliseconds to sub seconds). This first tier of the fog, designed for machine-to-machine interaction, collects, processes the data, and issues control commands to the actuators. It also filters the data to be consumed locally, and sends the rest to the higher tiers. The second and third tier deal with visualization and reporting (human-to-machine interactions), as well as systems and processes (machine-to-machine interactions). The time scales of these interactions, all part of the fog, range from seconds to minutes (real-time analytics), and even days (transactional analytics). As a result of this the fog must support several types of storage, from ephemeral at the lowest tier to semi-permanent at the highest tier. We also note that

[5] The smart traffic light node interacts locally with a number of sensors, which detect the presence of pedestrians and bikers, and measures the distance and speed of approaching vehicles. It also interacts with neighbouring lights to coordinate the green traffic wave. Based on this information the smart light sends warning signals to approaching vehicles, and even modifies its own cycle to prevent accidents. [18]

the higher the tier, the wider the geographical coverage, and the longer the time scale. The ultimate, global coverage is provided by the cloud, which is used as a repository for data having a permanence of months and years, and which is the bases for business intelligence analytics. This is the typical environment of reports and dashboards that display key performance indicators. [18]

Related Concepts and Technologies

The examples of fog computing in the previous section mentioned three keywords representing future trends in fog computing: Industry 4.0, smart cities, and smart grids. There are two technologies that significantly contribute to such application of fog computing: Internet of Things (IoT) and software-defined network (SDN).

IoT is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. The basic idea of this concept is the pervasive presence around us of a variety of things or objects – such as Radio-frequency Identification (RFID) tags, sensors, actuators, mobile phones, etc. – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbours to reach common goals. [20]

SDN is a new networking architecture that is designed to use standardized API to quickly allow network programmers to define and reconfigure the way data or resources are handled within a network. The use of an API allows network applications (such as email systems, cloud computing services, or telephony applications) to easily interface and reconfigure the network and its components (such as switches, racks of servers, virtual machines, and other end devices), or pull specific data, based on their particular requirements. [21]

1.2.2 Factory Cloud and Robot as a Service (RaaS)

Following the trend of the last years and also Industry 4.0 requirements, the factory of the future will have to meet requirements for a fully customized production with lot size one. Robots and machine tools thus need to be capable of fast reconfiguration. Acquisition and analysis of all possible process data becomes necessary. All sensors, actuators, and computing algorithms have to be connected together to achieve collection and usage of the data. In order to cope with the modified infrastructure of production systems, the control architecture of machines and robots will transform from a hierarchical to a flat and fully meshed setup. The so-called cyber-physical production system (CPPS) [22] should then be able to provide and use various services. [23]

Factory cloud consists of various cloud-based services of control systems as depicted in Figure 1.7, from factory management enterprise resource planning (ERP), through manufacturing execution system (MES) at the planning level, Supervisory Control and Data Acquisition (SCADA) at the control station level, to field programmable logic controller (PLC) at the cell level and computer numeric control (CNC) at the machine level. All these control systems are modularized and interconnected and their services, publicly accessible in the factory cloud, must be orchestrated into business and factory production processes. The integration of soft-PLC and robot controller (RC) into a real-time capable virtual machine leads to a virtual programmable logic controller (VPLC) and a virtual robot controller (VRC), respectively, as introduced in [23] and depicted in Figure 1.8.

Factory clouds have been typically implemented as private clouds because field-level systems require low-latency connections for exact control of attached machines. However, in the case of robots and their VRCs, it is suitable to publish their services globally and

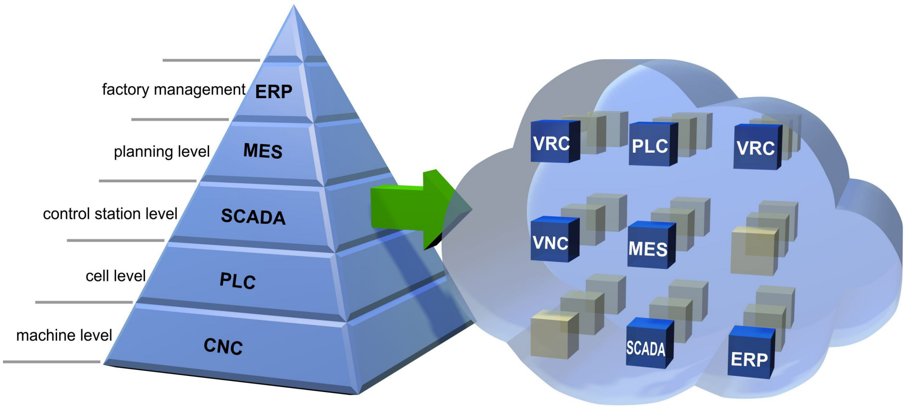


Figure 1.7: Modularization and virtualisation of factory control components (adopted from [23]).

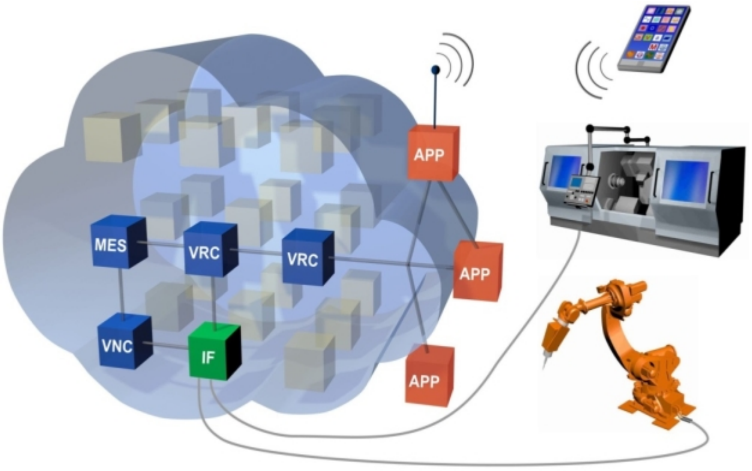


Figure 1.8: Factory cloud with interfaces to robots, machine tools and services (adopted from [23]).

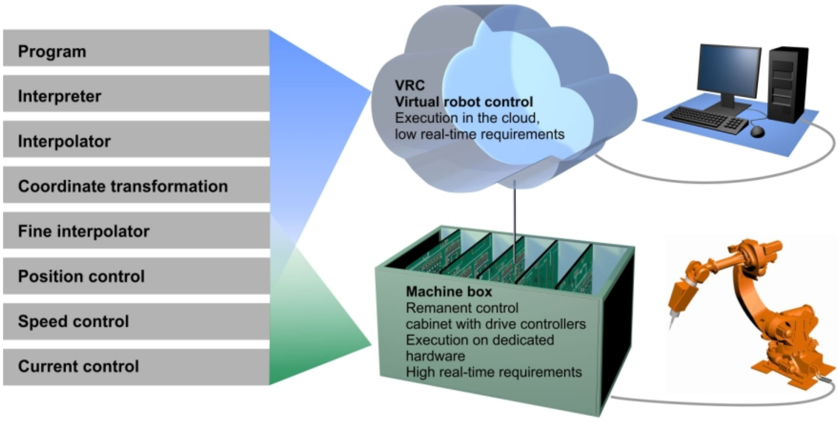


Figure 1.9: Transferring motion functions from control cabinet to VRC depending on real-time requirements (adopted from [23]).

make them accessible in a public cloud, e.g., to monitor production by available metrics and produce and analyse corresponding key performance indicators (KPIs). In [24], a concept of Robot as a Service (RaaS) is introduced to address the above mentioned issue.

The RaaS service model enforces the design and implementation of a robot or a device to be an all-in-one service-oriented architecture (SOA) unit, that is, the unit includes services for performing functionality, service broker for discovery and publishing, and applications for client's direct access. Contrary to previous designs of SOA robots where the robot is an application that uses services from a remote back-end computer, RaaS concept gives the robot unit much more power and capacity, so that it can qualify as a fully self-contained cloud unit in the cloud computing environment. [24]

In [23], the authors split VRC into two cloud services to separate functions with low real-time requirements from functions with high real-time requirements that are necessary for position, speed, and current control of robotic devices. In this approach, a new VRC implements cloud services for the functions with low real-time requirements, while the functions with high real-time requirement are implemented as edge cloud services according to the RaaS service model. In this way, the new VRC cloud services can be moved into a public cloud and the original private cloud can be dynamically extended with public resources as depicted in Figure 1.9.

1.2.3 Big Data, Fast Data, and Data as a Service (DaaS)

Data as a Service (DaaS) is a type of cloud computing services that provides data on demand. A DaaS typically exposes its provided data to consumers through API, either for the consumer to download or query data from different data assets. By using DaaS, consumers do not need to fetch and store giant data assets and search for the required information in the data asset. Instead, they simply find a suitable DaaS that provides the data asset having the desired information and call the corresponding API to retrieve the data. With recent developments in cloud computing, it has become easier to build DaaS that provide bigger data assets at lower costs on the clouds. [25]

With fog computing, factory clouds, etc., amount of devices implementing their cloud services that are able to act according to DaaS service model as data-sources is rapidly increasing. Moreover, also another cloud services produce a large amount of data as their results or values of their monitoring metrics. Finally, there is a lot of public and private data-sources available in organisations as well as on the Internet that together contain a very large volumes of various data growing at an exponential rate. Such data are typically heterogeneous, of multiple data types, and highly dynamic, and can be described as Big data and their processing must be performed by specific Big data technologies. According to [26], Big data technologies describe a new generation of technologies and architectures, designed to economically extract value from very large volumes of a wide variety of data, by enabling high-velocity capture, discovery, and/or analysis. Therefore, Big data can be characterised by what is often referred to as a multi-V model according to [27]:

- *Variety* represents various data types of Big data that can be structured (with formal schema and data models), unstructured (no pre-defined data model), semi-structured (lacks a strict data model structure), or mixed (various types together).
- *Velocity* refers to the high rate at which the data is produced and processed.
- *Volume* defines the large amount of data.
- *Veracity* refers to how much the data can be trusted given the reliability of its source.
- *Value* corresponds the monetary worth that a company can derive from employing Big data computing.

Considering data velocity, it is noticed that, to complicate matters further, data can arrive and require processing at different speeds: in batches at given time intervals; in near real-time at frequent small time intervals; in real-time with continuous input, processing, and output; and in streams of data flows. Whilst for some applications, the arrival and processing of data can be performed in batch, other analytics applications require continuous and real-time analyses, sometimes requiring immediate action upon processing of incoming data streams. [27]

Big data with focus on velocity are known as Fast data, i.e., high-speed real-time and near-real-time data streams. Prime examples include sensor data streams, real-time stock market data, and social-media feeds such as Twitter, Facebook, YouTube, Foursquare, and Flickr. Numerous applications must process Fast data, often with minimal latency and high scalability, and common Big data processing approaches, such as MapReduce in Apache Hadoop, may not be well suited for these applications. For example, an application that monitors the Twitter Firehose for an ongoing earthquake may want to report relevant information within a few seconds of when a tweet appears, and must handle drastic spikes in the tweet volumes. [28]

Big data processing must be done in distributed computing environments by parallel algorithms to be able to address high velocity and volume characteristics of Big data. Therefore, Big data processing is often performed in cloud computing, usually in IaaS and PaaS service models where cloud providers offer distributed IT infrastructure (e.g., computation clusters) or services of Big data processing platforms such as Apache Hadoop or Apache Storm. However, it is also possible to provide general or customised services for Big data analytics in the SaaS service model. In these cases, there can emerge new "Big Data . . . as a Service" service models as depicted in Figure 1.10.

1.3 Cloud Computing in Practice

In past years, cloud computing has been a fast growing industry. There are many cloud computing providers and another new providers are emerging with new topics to address such as Big data, IoT, etc. The OpenCrowd Cloud Taxonomy [30] demonstrates cloud

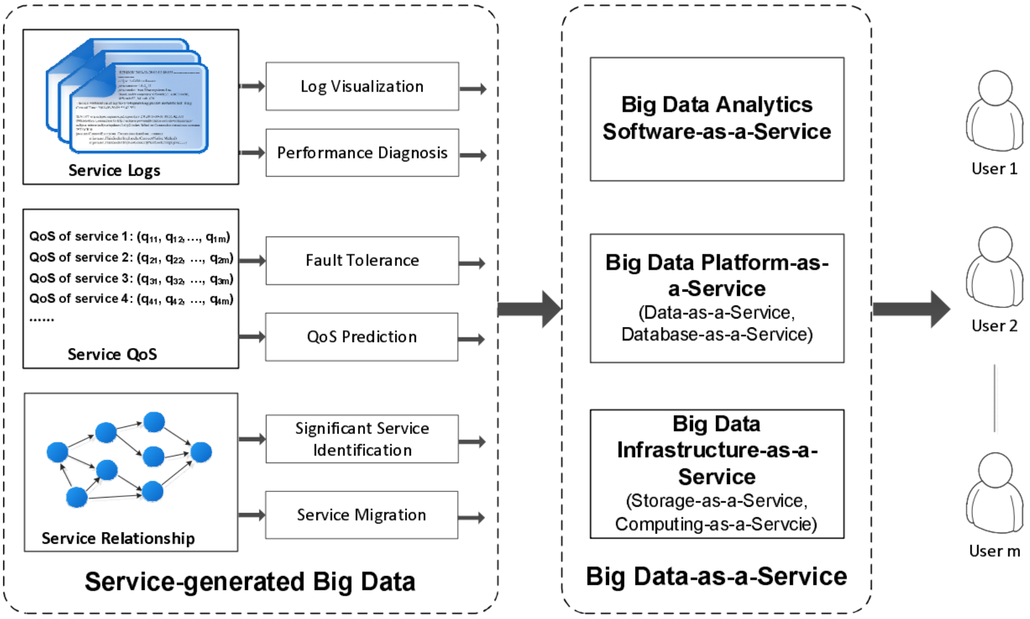

Service Logs
Log Visualization
Performance Diagnosis
QoS of service 1: (q11, q12, ..., q1m)
QoS of service 2: (q21, q22, ..., q2m)
QoS of service 3: (q31, q32, ..., q3m)
QoS of service 4: (q41, q42, ..., q4m)
......
Service QoS
Fault Tolerance
QoS Prediction
Service Relationship
Significant Service Identification
Service Migration
Service-generated Big Data
Big Data Analytics Software-as-a-Service
Big Data Platform-as-a-Service (Data-as-a-Service, Database-as-a-Service)
Big Data Infrastructure-as-a-Service (Storage-as-a-Service, Computing-as-a-Servcie)
Big Data-as-a-Service
User 1
User 2
User m

Figure 1.10: Overview of service-generated Big data and Big Data as a Service (adopted from [29]).

computing SW and solutions available today across IaaS, PaaS, and SaaS service models (see Figure 1.11). Thorough analysis and comparison of these cloud computing SW and solutions will be subject of next chapters.

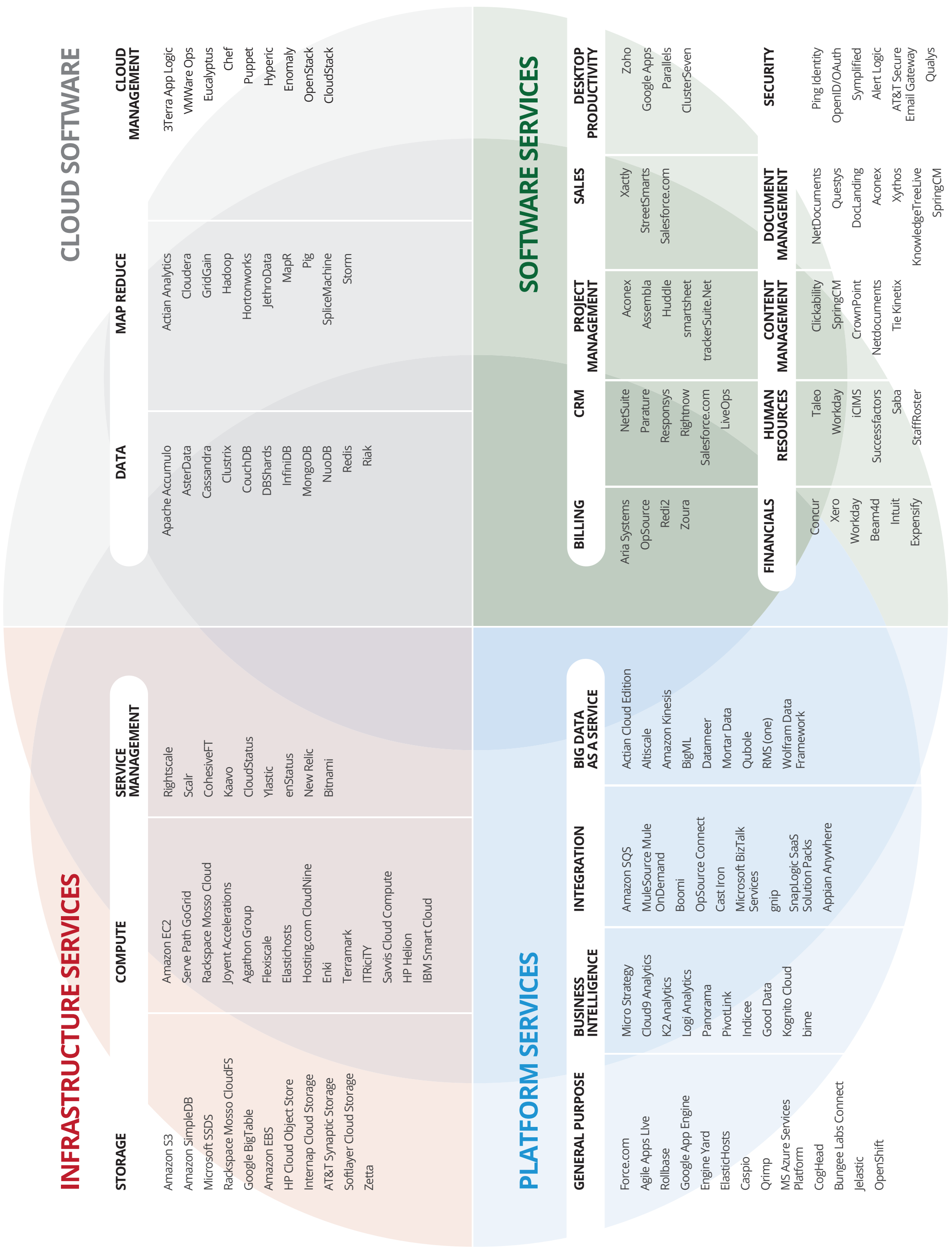


Figure 1.11: The Cloud Taxonomy by OpenCrowd (adopted from [30]).

2 Cloud Computing in Manufacturing Industry

Cloud computing brings new opportunities to manufacturing industry. The manufacturing organisations that successfully utilised modern technologies in production are ready to adopt cloud computing technologies too and cloud computing is rapidly moving from early adopters to mainstream organizations. Moreover, globalised manufacturing organisations are starting to act according to Design Anywhere, Manufacture Anywhere (DAMA) philosophy [31] which demands the ability to move their design and manufacturing facilities at short notice to respond to changes in the market.

Adoption of the DAMA approach brings another reason for cloud computing because where multiple sites are involved, the complexity of information management needed for successful product introduction rises exponentially and there is special need for information technology (IT) systems and infrastructure connecting various parts of the enterprise, such as manufacturing resource/requirements planning (MRP), enterprise resource planning (ERP), engineering resources planning and customer relationship management (CRM), as well as for vertical integration between their components as depicted in Figure 2.1.

Smart manufacturing with cloud computing and cloud manufacturing are two types of cloud computing adoptions in the manufacturing sector [32]. The first one is manufacturing with direct adoption of some cloud computing technologies, where the adoption is typically centred on the Business Process Management (BPM) applications such as HR, CRM, and ERP functions, while the second one is the manufacturing version of cloud computing. The cloud manufacturing (CMfg) is defined in [32] by mirroring National Institute of Standards and Technology (NIST) cloud computing definition[1] of cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable manufacturing resources (e.g., manufacturing software (SW) tools, manufacturing equipment, and manufacturing capabilities) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Contrary to the smart manufacturing with cloud computing, which usually provides services in Software as a Service (SaaS) or Platform as a Service (PaaS) service models, the CMfg is more technologically oriented and thus, it typically implements lower-level service models such as PaaS or Infrastructure as a Service (IaaS). For an example of the CMfg technologies see Section 1.2.2.

This chapter will discuss both smart manufacturing with cloud computing and CMfg with focus on their applications in automotive and electronics industry.

2.1 Cloud Computing in Automotive/Electronics Industry

The globalisation of the electronics industry has brought many challenges for companies that produce electronic products, not least of which is how to share information across

[1] The NIST definition of cloud computing is in Section 1.1.

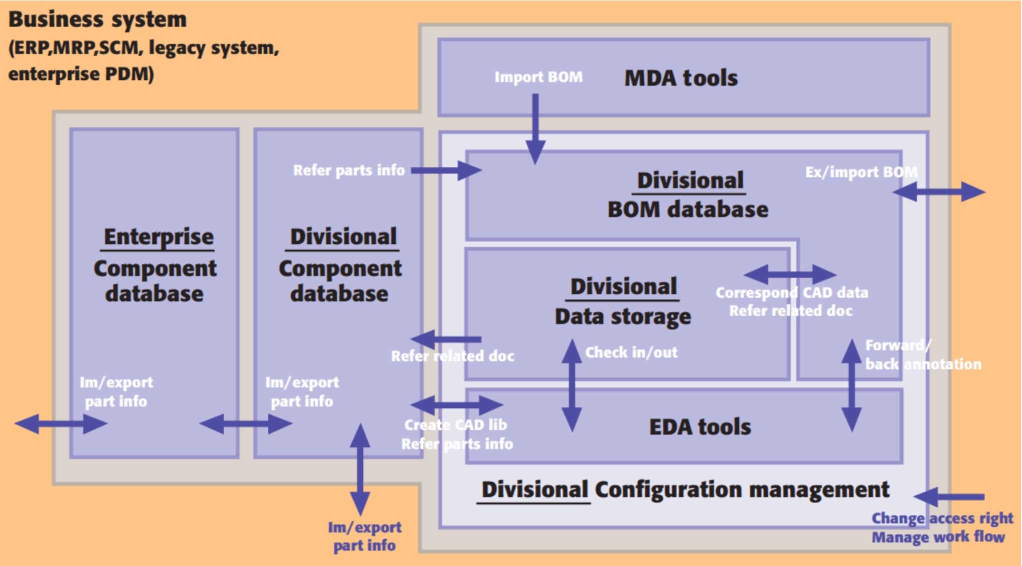


Figure 2.1: Structure of a system to implement the DAMA philosophy (adopted from [31]).

the enterprise and with design and manufacturing partners who may be located anywhere across the globe in accordance with the DAMA philosophy. Without effective sharing of information, the enterprise becomes confused, slow to respond and, ultimately, uncompetitive. Therefore, electronic product design and development cannot work in isolation. The necessary links between component databases, bills of material, design tools, design process management, mechanical design tools and product data are already complex. It is still true that the communication between schematic and layout engineers are often imperfect; the designers involved can be sitting at adjacent desks and passing scraps of paper to each other. [31]

The similar reasoning as described above by [31] can be applied also in automotive industry. Following automotive value chain with individual stages for design, supply, assembly, retail, and after-market services, there are many opportunities for cloud computing in automotive industry [33]. These opportunities, together with possible threats will be discussed in the following sections. Before presenting the opportunities, it is necessary to provide a critical review of recent development and future trends of cloud computing in the automotive (and electronics) industry for both smart manufacturing with cloud computing and CMfg.

2.1.1 Smart Manufacturing with Cloud Computing

The smart manufacturing with cloud computing is typically considered from business perspective as it utilises SaaS service providing ready-to-use solutions for enterprise management or PaaS/IaaS services for better deployment of already existing technical solutions such as enterprise information systems or individual databases, web presentations and web/e-commerce portals for employees, business partners, and customers. From this business perspective, organisations in the automotive or electronics industries need the same cloud services as organisations outside of this fields – they require BPM applications such as HR, CRM, and ERP functions. Moreover, there are special applications such as manufacturing planning, collaborative supply chain management, collaborative design systems, simulation tools, etc.

The cloud computing can bring the following technologies that help to meet the business requirements:

Business Process Management (BPM) – SaaS

Large companies as well as advanced SMEs have to monitor and control their business processes. A BPM system typically helps to manage a business structure of an organisations and control consistency and security of business processes for their participants. BPM applications include CRM, workforce performance management (WPM), ERP, business activity monitoring (BAM), e-commerce portals and others. In cloud, BPM systems are usually provided as SaaS which enhances flexibility, deploy-ability and affordability for complex enterprise applications [34]. In many cases, the moving of BPM into cloud as SaaS may enable better monitoring and control of managed business processes and increase re-usability of business processes and their fragments. BPM in the cloud can help the enterprises to maximize their profits, or to introduce new intelligent/innovative business processes. For example, the introduction of situational business processes [35] helps to adapt the enterprises to completely new business situations: new initiatives, new campaigns, and new projects.

Examples of BPM in cloud can be IBM BPM on Cloud[2], NetSuite services[3], or Salesforce[4].

Data Migration and Load Balancing – PaaS/IaaS

The issue of distributing information to web users in an efficient and cost-effective manner is a challenging problem, especially, under the increasing requirements emerging from a variety of modern applications, e.g., voice-over-Internet Protocol (IP), and streaming media. More and more applications (such as e-commerce) are relying on the Web but with high sensitivity to delays. A delay even of a few milliseconds in a Web server content may be intolerable. Content distribution networks (CDNs) have been proposed to meet such challenges by providing a scalable and cost-effective mechanism for accelerating the delivery of the Web content [36].

While CDNs can be considered as PaaS/IaaS cloud services, data migration to cloud requires more advanced services that ensure the following goals [34]:

- *No data loss*: The system must ensure with a high probability that data will not be lost permanently.
- *High availability*: Data must be available to users/owners when they want the data with a reasonably high probability, though some occasional temporary outages are acceptable.
- *High performance*: The system should not perform significantly worse than the current usual alternatives notably NFS.
- *Scalability*: The system must scale to large numbers of clients, large numbers of storage "nodes", large aggregate storage spaces, etc.
- *Cost efficiency*: Since there are existing solutions to buy large, reliable storage, the system must be inexpensive in hardware (HW), SW, and maintenance.

[2] `https://www.bpm.ibmcloud.com/`

[3] `http://www.netsuite.com/`

[4] `https://www.salesforce.com/eu/`

- *Security*: The system must be able to match the confidentiality, data integrity, and authorization standards expected by users. This is particularly challenging given that data will be stored on the remote machines of cloud providers.

The most of these goals are met by popular vendors of Storage as a Service (StaaS) services that can be categorised under the PaaS model. However, in some cases, such as for the security goal, it may be necessary for an enterprise organisation to deploy their own virtualised SW stacks into cloud under IaaS services (the security concerns will be discussed in more details in Section 2.3). Actually, StaaS and CDNs can be suitable also in the cases of custom solutions running on IaaS services, to add load-balancing and failover due to the limited resources, failures, operation maintenance downtimes, etc.

An example of CDNs solution can be Akamai[5] or Amazon CloudFront[6]. In the case of SaaS, popular cloud service providers are Amazon Simple Storage Service (S3)[7] or Google Cloud Storage[8].

Virtualisation – PaaS/IaaS

Virtualisation refers to the abstraction of logical resources away from their underlying physical resources in order to improve agility, flexibility, reduce costs and, thus, enhance business value. Handling a number of virtualisation machines on the top of operating systems and evaluating, testing servers and deployment to the targets are some of the important concerns of virtualisation. The basic elements of the hyper-visor include central processing unit (CPU), memory management, and input/output (I/O) which provide the greatest performance, reliability and compatibility. Virtualisation in the cloud includes server virtualisation, client/desktop/application virtualisation, storage virtualisation by Storage Area Network (SAN), network virtualisation by virtual private network (VPN) and software-defined network (SDN), and service/application infrastructure virtualisation. Virtualisation is therefore well suited to a dynamic cloud infrastructure, because it provides important advantages in sharing of cloud facilities, managing of complex systems as well as isolation of data/application. Additionally, the significant idea is to ensure whether the data centres are locked or not into a particular operating system environment through their choice of a virtualisation. [36]

For enterprise organisations, the virtualisation is probably the most interesting feature of cloud computing, as it allows them to easily move their existing "legacy" systems into cloud, allow better scalability and reduce costs for HW (and system SW) maintenance. This is suitable especially for manufacturing industry where many legacy systems usually exist that cannot be replaced or reimplemented for various reasons (due to licences, proprietary parts, dependencies on third-party business/government systems, deprecated technologies, high costs, etc.). In many cases, such systems can be moved without any further modifications into virtualised environments on the assumption that the virtualisation sufficiently emulate the original native run-time environment of the migrated systems.

From the point of view of a user of cloud services, the virtualisation can be provided as either PaaS or IaaS solution. In the case of PaaS, a cloud provides individual virtual SW components that can be used to build the virtualised systems (e.g., a virtual Apache HTTP Server or a virtual MySQL/Oracle database that behave the same way as their

[5] https://www.akamai.com/

[6] https://aws.amazon.com/cloudfront/

[7] https://aws.amazon.com/s3/

[8] https://cloud.google.com/storage/

physical instances). In the case of IaaS, the virtualisation is done at HW or operating-system level where the virtualised system is deployed or installed, respectively, in the same way as for physical HW or physical installation of the operating system. An example of the PaaS-type virtualisation can be Heroku Cloud Application Platform[9], while the IaaS-type virtualisation would be Amazon Elastic Compute Cloud (EC2)[10].

Monitoring and Big Data Analytics – SaaS/PaaS

According to McKinsey&Company, manufacturing is already an intensive user of Big data. Massive data sets are used to discover new patterns, perform simulations, and manage complex systems in real-time. Manufacturing stores more data than any other sector – an estimated two exabytes in 2010. By enabling more sophisticated simulations that discover glitches at an early stage, Big data has helped Toyota, Fiat, and Nissan cut the time needed to develop new models by 30 to 50%. [37]

In modern manufacturing industry, data are generated by monitoring of machines and devices, cloud-based solutions, business management, etc., and these data need to be processed in real-time as well as stored for further analyses. Besides cloud computing solutions for BPM, data storage, virtualisation, etc. as described above, Big data require specific techniques and methods for their storage, processing, analysis. There are cloud computing service models particularly focused on Big data, as it was described in Section 1.2.3, however, Big data analytics in manufacturing industry has its particular goals and applications, such as virtual factory (VF) for a simulation of a real factory, or prognostics and health management (PHM) of cyber-physical systems—production machines. Moreover, there are Big data from business and production process monitoring that are processed for BAM and for decision-making by human operators of rules engines to optimize production.

Virtual factory (VF) is described in [38] in four dimensions as:

- *A simulation of a real factory* for simulated networked planning and control of production processes with the aid of digital models, which has been adopted by many manufacturing companies. For example, Ford Motor Company has implemented its virtual factory systems of European facilities to improve assembly-line efficiency by previewing and optimizing systems using simulations and virtual environments, or Volvo Group Global has developed tools to create virtual factories to validate changes before they are introduced into an actual plant. Decision makers can run several thousands of simulations of different concepts to evaluate process flows, robots movement, and people's risks and stress before the plant is built.

- *A virtual organization* defined as linking multiple real factories at different locations in a network for manufacturing a product for joint process monitoring, problem identification and solving, and performance metrics communication and sharing among participating companies of a virtual factory.

- *A virtual reality representation* as a 3D environment that is designed for simulation, visualization, communication, and collaboration using networked, real-time 3D and 2D information for the factory and its processes. The 3D representation can be used to perform process monitoring, virtual inspections, inventory tracking, customer tours, education, and training, to access information such as design drawings, process plans, process and equipment statistics, and other manufacturing knowledge.

[9] `https://www.heroku.com/`

[10] `https://aws.amazon.com/ec2/`

- *An emulation facility* for safe simulations of real-world production processes, especially of experimental modifications of their production activities, using discrete event simulation (DES) modelling of the activities in a virtual factory with data provided by real-world sensors and the processes controlled by real-world control systems.

Software for product, process, and system design, simulation, and visualization in a virtual factory is provided by major vendors of factory automation such as Dassault Systemes[11], Siemens PLM[12], and PTC[13].

Prognostics and health management (PHM) provides insights into future equipment performance and estimation of the time to failure of machines in manufacturing, to reduce the impacts of these uncertainties, and give users the opportunity to proactively implement solutions to prevent performance loss of the manufacturing system [39]. According to [40], an algorithm has to be established to track the changes of a machine status, infer additional knowledge from historical information, apply peer-to-peer comparison and pass the outputs to the next level. The change of a machine status can be defined as a dramatic variation in machine health value, a maintenance action, or a change in the working regime.

During the life cycle of a machine (an asset), snapshots of the machine status are accumulated and used to construct the time-machine history which will be used for peer-to-peer comparison between machines. Then, a pattern matching algorithm is used to look back in historical time machine records to calculate the similarity of current machine behaviour with former assets utilisation and health. Finally, predicting remaining useful life of assets helps to maintain just-in-time maintenance strategy in manufacturing plant. In addition, life prediction along with historical time machine records can be used to improve the asset utilisation efficiency based on its current health status. Historical utilisation patterns of similar asset at various health stages provide required information to simulate possible future utilisation scenarios and their outcome for the target asset. Among those scenarios, the most efficient and yet productive utilisation pattern can be implemented for the target asset. [40]

2.1.2 Cloud Manufacturing

According to [41], the CMfg is based on the idea of Manufacturing as a Service (MaaS), which is the seamless and convenient sharing of a variety of different kinds of distributed manufacturing resources as services, for all phases of a product development life-cycle. There are mainly three types of participants or users in a CMfg system: (1) a consumer with a manufacturing demand, (2) a provider with resources to satisfy this demand, or parts of it, and (3) an operator in between, orchestrating the organisation of demands and available resources, for a successful match between demands and resources. The provider's resources in CMfg are of two types: physical manufacturing resources and manufacturing capabilities (sometimes also referred to as "abilities").

Physical resources can be either hard (such as manufacturing equipment, computers, networks, servers, materials, facilities for transportation and storage, etc.) or soft (e.g. applications, product design and simulation SW, analysis tools, models, data, standards, human resources such as personnel of different professions and their knowledge, skill, and experience, etc.). Manufacturing capabilities are intangible and dynamic resources that represent an organisation's capability of undertaking a specific task or operation with

[11] `https://www.3ds.com/`

[12] `https://www.plm.automation.siemens.com/`

[13] `https://www.ptc.com/`

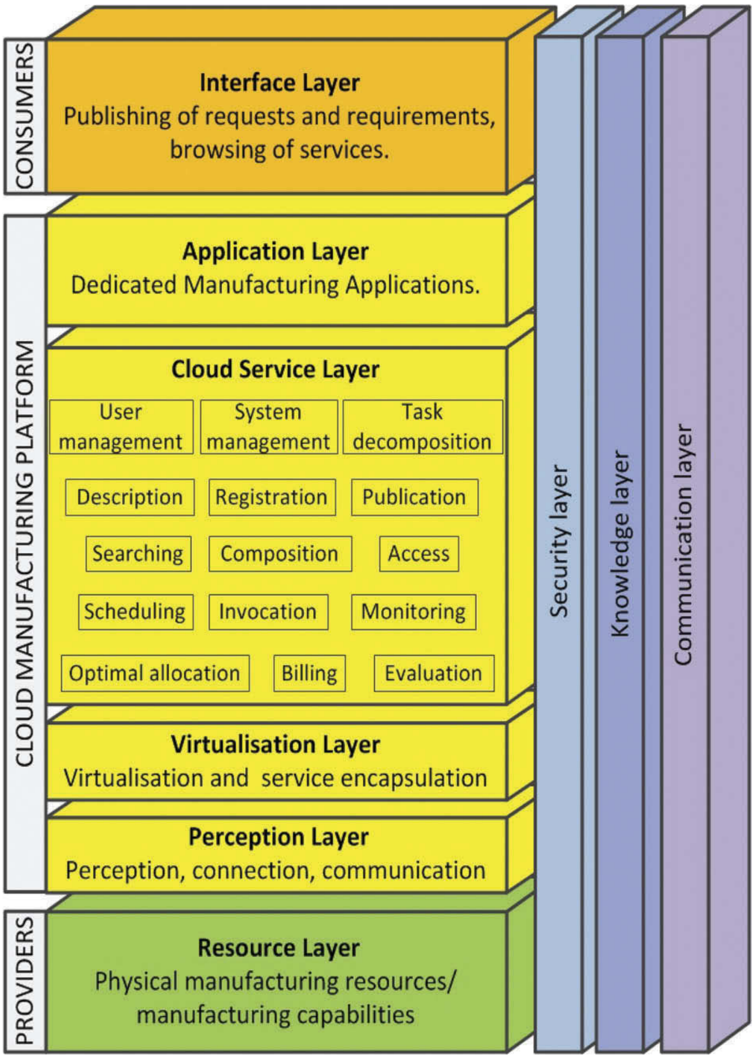


Figure 2.2: Cloud manufacturing (CMfg) concept architecture (adopted from [41]).

competence, using physical resources (e.g. performing product designs, simulations, manufacturing, management, maintenance, communication, etc.). It is the manufacturing capabilities that determine whether the requirements can be achieved by the manufacturing resources during product development. Both manufacturing resources and capabilities are virtualised and encapsulated as CMfg services, which are on-demand, configurable, and self-contained services, to fulfil a consumer's needs. Manufacturing SW, applications, and infrastructures can thus be provided as services in CMfg, in a similar manner as computing resources are being provisioned in different structures in comparison criteria (CC) [41].

Above the physical manufacturing resources and the manufacturing capabilities, there is a CMfg platform with several layers responsible for their sensing (discovery and connection), virtualisation (providing them with interfaces), management (encapsulating them as cloud services), aggregation and composition (into manufacturing services in the cloud), and publishing to consumers. For all these layers, security enforcement, knowledge sharing and management, and communication must be ensured by supporting layers, as depicted in Figure 2.2.

Nowadays, CMfg is the subject of ongoing research and many research initiatives, projects, and consortiums with both academic and industrial participants have been established to propose and evaluate CMfg concepts in practice. For example, the following recent initiatives maybe interesting from point of view of automotive/electronics manufacturing in European Union[14]:

- ManuCloud (a distributed cloud product specification and supply chain manufacturing execution infrastructure) [42]
- Diversity (cloud manufacturing and social software based context sensitive product-service engineering environment for globally distributed enterprise) [43]
- CREAM (cloud-based rapid elastic manufacturing) [44]
- SMARTER (sustainable manufacturing adaptive services with cloud architectures for enterprises) [45]
- cloudSME (simulation for manufacturing & engineering) [46]

There are also many cloud services vendors that declare themselves as CMfg providers, for example NetSuite[15], Plex [16], KeyedIn[17], Scytex[18], Hai[19], Rootstock Software[20], QAD[21], Hudman[22], and others. However, despite of their declarations, the most of the vendors do not actually provide CMfg services but smart manufacturing solutions with cloud computing, usually as an ERP SaaS.

Moreover, there are also individual open or proprietary technologies and standards that make CMfg possible by establishing a standardised communication bus and interfaces of machines to include them as Machine as a Service cloud services, for example, MTConnect[23], OCCI[24], UN/EDIFACT[25], ebXML[26], MyOpenFactory[27], RosettaNet[28], SEMI EDA/Interface A[29] and others.

Selected CMfg solutions for automotive/electronics industry will be discussed in Chapter 3.

2.2 Opportunities and Threats of Cloud Computing

Implementation of a manufacturing cloud from scratch and transition from well-established manufacturing or business systems to their representation in cloud bring many opportunities as well as threats for a manufacturing organisation. In this section, the opportunities and the threats will be identified and their possible effects and countermeasures will be analysed, respectively, based on the previous text and referred publication, e.g., [47, 48, 33, 41]. Security threats are subjects of Section 2.3.

[14] another exhaustive list of research trends, publications, and initiatives is provided by [41]
[15] http://www.netsuite.com/portal/industries/manufacturing.shtml
[16] https://www.plex.com/
[17] https://www.keyedin.com/manufacturing/
[18] https://scytec.com/dataxchange-overview/
[19] http://www.hai.nl/
[20] http://www.rootstock.com/manufacturing-cloud-erp/
[21] https://www.qad.com/cloud
[22] https://www.hudmansolutions.com/
[23] https://www.mtconnect.org/
[24] https://occi-wg.org/
[25] http://www.unece.org/trade/untdid/texts/unredi.htm
[26] http://www.ebxml.org/
[27] https://www.myopenfactory.com/
[28] https://resources.gs1us.org/RosettaNet
[29] https://www.cimetrix.com/InterfaceA

2.2.1 Opportunities in General

O1 – Low initial investment: One of the significant opportunities of cloud computing lies in its potential to help starting organisations reap the benefits of IT in their business without the significant upfront investments. Instead of a big initial investment which was necessary before cloud computing to buy an information or manufacturing system SW and to build a suitable IT infrastructure, the cloud computing requires significantly lower initial investment, especially in the case of SaaS that can be used without any preparation. The cloud services are consumed on-demand and paid per usage (a "pay-as-you-go" billing method). The low initial investment can make sense for small businesses that can exploit high-end applications like ERP SW or business analytics typically provided as SaaS, as well as for large organisation that can try different innovations without high expenses.

O2 – Outsourcing and IT service management: To provide IT services in-house by an IT department of a manufacturing organisation means to implement IT service management, from development of new IT services according to changing needs of end-users, through transition of these services in practice, to their maintenance and improvement during IT operation management. While the IT service management processes are quite well described in various well-established methodologies, e.g., in IT Infrastructure Library (ITIL) or ISO/IEC 20000[30], their implementation requires specialised staff, processes, and infrastructure components (e.g., for backup/restore, hot-swapping of erroneous IT components, configuration management, etc.) that must be well-integrated into the organisation. Contrary to that, from the end-user perspective, a well-defined cloud computing solution is easy to maintain without the extra IT knowledge and assets.

O3 – Mashups: The ability to quickly combine data or functionality from two or more external sources to create a new "mashup" service in originally unintended ways represents another opportunity in cloud computing. The cloud computing better addresses needs of agile development and agile business as it is quite easy to take several cloud services and utilise them as components of a new cloud in short notice rather than building applications from scratch. For examples, one can take several special private-cloud Data as a Services (DaaSs) and a general public-cloud Big Data Analytics as a Service and quickly build a hybrid-cloud service to analyse real-time data. Without cloud computing, such a use case would be difficult to implement without special SW, IT infrastructure, and big investments.

O4 – Better IT architecture: To build a good, extensible, and scalable IT architecture is challenging for an IT organisation and may be very difficult for a non-IT manufacturing organisation. With additional modifications of an IT system emerging during its life-time, its architecture becomes "accidental". According to [49], an intentional architecture is explicitly identified and then implemented; an accidental architecture emerges from the multitude of individual design decisions that occur during development, only after which can we name that architecture. This will certainly increase complexity of the architecture and its maintenance costs, and can cause a degradation of the architecture resulting into an erroneous system. This is usually not the case of cloud computing architecture where interfaces and dependencies between cloud services must be well-defined and it is much easier to rebuild or throw away the whole architecture or its part (re-development costs are minimal, in comparison with non-cloud solutions).

[30] `http://itil.co.uk/` and `https://www.iso.org/standard/51986.html`, respectively

O5 – Scalability: The scalability is an ability to up-scale or down-scale a system easily on demand, as quickly and effectively as possible, that is in controlled way and with minimum costs. This is quite problematic as to be able to scale down or up, the system must use more resource than needed in the case of the scale-down, or have these at its disposal in the case of the up-scale. In both cases, those resources are not utilised effectively. Therefore, the high scalability is considered to be a great advantage of cloud computing where the up-scale or down-scale of cloud services can be done immediately and a customer is always paying just as much money as it is the current consumption of the ordered cloud services.

O6 – Energy efficiency (green IT): Moving to the cloud will allow organizations to reduce their IT infrastructure. Virtualised IT infrastructure still depends on physical HW, however, this HW is located at cloud providers where it can be optimally utilised. Moreover, in the case of modification of the IT infrastructure due to requirements of new applications or just to up-scale or down-scale the current application, it is much cheaper in term of environmental resources to perform the modification on virtual than on physical IT infrastructure. Finally, transporting computing services from producers to consumers is more effective than doing the same with electrical energy.

2.2.2 Opportunities for Automotive/Electronics Manufacturing

O7 – Connected vehicle: Modern cars are equipped with a high amount of electronic systems with sensors that generate a lot of diagnostic and transactional data. A vehicle, if connected, can upload this data into an external data storage of a manufacturer or a service centre for further analyses. Currently, the upload is performed usually during annual vehicle inspections or maintenance. With cloud computing and a vehicle connected to a cloud, the data upload can be continuous and besides common analytics for individual vehicles, their manufacturers can apply Big data processing techniques (e.g., data mining) to get further insights they need to enhance services in areas such as CRM, marketing, quality, customer services, after-market services, or to perform research and development. Moreover, with fog computing, the vehicle itself or its electronic modules can act as edge cloud services and participate in the cloud (with necessary safety measures), e.g., for telematics, remote digital maintenance, or to provide infotainment services. Actually, the cloud computing is probably only possible way how to implement efficient data- and service-exchange between the high amount of devices.

O8 – Agile manufacturing (flexibility): High and controlled agility is desired feature in manufacturing. In [50], the agile manufacturing should ensure: high quality and highly customised products; products and services with high information and value-adding content; mobilisation of core competencies; responsiveness to social and environmental issues; synthesis of diverse technologies; response to change and uncertainty; and intra-enterprise and inter-enterprise integration. CMfg, as defined in Section 2.1.2, can meet most of these requirements, for example, in the form of cloud robotics which brings better monitoring, automatic optimisation, and faster reconfiguration of robotics product lines.

O9 – Better monitoring (transparency): Besides better control and integration, the manufacturing cloud enables also better monitoring. Individual machines participating in a production can be accessed as cloud services according to Machine as a Service and DaaS models. Data loaded from these services periodically in batches or received in data-streams can be aggregated and filtered when passing through another services in accordance with fog/edge computing concepts and finally, processed as Big data by analytical tools and systems, for example, by another services in Big Data (Analytics) as a Service (see Section 1.2.3). This allows better continuous computation of various metrics (e.g., to observe progress of operations or health of the machines) and also high-level key performance indicators (KPIs).

2.2.3 Threats

T1 – Dependency and vendor lock-in: Currently, the concept of cloud computing lacks standardisation. There are many proprietary and open-source solutions and although many of them build cloud architectures on open standards, such as Web services, there is no compatibility of resulting systems which would allow easy migration from one to another. With this "vendor lock-in", there is a legitimate concern that data or functionality in cloud may be harmed, for example, if a cloud provider goes bankrupt, or goes off-line due to attacks or serious flaws in maintenance[31]. Also GNU founder Richard Stallman warns that "Cloud computing is a trap" [52]. According to [47], a cloud computing service by a single company is in fact a single point of failure and even if the company has multiple data centres in different geographic regions using different network providers, it may have common SW infrastructure and accounting systems, or the company may even go out of business – we believe the only plausible solution to very high availability is multiple cloud computing providers.

T2 – Backlash from entrenched incumbents: As many IT departments of larger corporations can view cloud computing as a threat to their corporate IT culture in terms of data security, IT audit policies, etc., or just in terms of job security [48], they can reject the new technology of cloud computing requiring a change in well-established structures and processes.

T3 – Data lock-in, data confidentiality, and shared reputation: Another consequence of the lack of standardisation in cloud computing can be possible data lock-in. Cloud customers cannot easily extract their data and programs from one site to run on another which is preventing some organizations from adopting cloud computing [47]. Moreover, there is a question of data ownership. The data that was loaded by a customer into a service cloud (e.g., in a SaaS model) belongs to the customer, however, they are physically located in IT infrastructure of the service provider. The service provider may, in some cases, access and use the data for his/her purposes (e.g., for marketing or advertisement as is often the case of free cloud services provided by Google, etc.), may not be able to protect the data from possible leaking out (e.g., due to an unauthorised access if attacked), or must store and take care of data with legal measures (e.g., provide access to law enforcements agencies according to a particular jurisdiction, such is in the case of the United States of America (USA) PATRIOT Act[32]). Therefore, it may not be acceptable for some organisations to store their data in cloud (or to transport their data through cloud-based services, which is even more restricting). Moreover, there is a problem of reputation sharing where one customer's bad behaviour can affect the reputation of others using the same cloud IT

[31] For example, GitLab cloud service providing a Git repository version control system for tracking changes and coordinating team work in SW development faced a massive backup failure after an accidental production data deletion incident [51] that resulted into data-loss despite of the open-source standardised and distributed Git technology.

[32] https://www.justice.gov/archive/ll/highlights.htm

infrastructure, as described in [47], which may result into blacklisting of IP addresses or a data loss or leak due to an investigation of the incident by law enforcements agencies.

T4 – Non-transferable responsibility: The cloud computing services are usually provided as outsourcing. Moreover, it may be difficult to implement the services as insourcing in a public or hybrid cloud, especially for SaaS where all underlying levels (a platform and an infrastructure) are hidden inside the service and cannot be controlled or extracted and operated by the customers. Yet, in same case, it may be critical for a company to operate its services in-house, for example, for security or legal reasons, or just to prevent possible disclosure of well-protected organisational know-how. In these cases, for the point of view of the customer, the only suitable cloud-computing service model is IaaS with massive encryption for virtualisation containers, storage, and networking.

T5 – Data transfer bottlenecks: Great benefit of cloud computing is better scalability. It is not a problem to scale up or down on demand to meet a current or an expected load. However, the scalability in cloud computing means the ability scale up or down resources/services in cloud, not the scalability of connection links between those services and their customers. This fact must be well-understood and take into account when huge data transfers can be expected between cloud service providers and consumers. As suggested by [47], cloud users and cloud providers have to think about the implications of placement and traffic at every level of the system if they want to minimize costs (as the data transfer costs can be more expensive than data placement).

T6 – Performance unpredictability in multi-tenant environments: In multi-tenant virtualised environment, a shared pool of common resources is utilised to serve requests of all users without affecting each other – a single instance of each resource (e.g., a physical HW) serves multiple groups of users (tenants) to run particular services (e.g., to run an operating system on a virtualised HW provided as an IaaS service). The users/customers have guaranteed a particular level of provided cloud services in their Service Level Agreements (SLAs), e.g., a storage capacity or a response time, however, the real level of such services is usually higher than agreed most of time but varying for the minimal agreed to maximal available according to the total consumption rate of the services by all users (the service load). From the point of view of a single user/customer, the actual level of a service is difficult to predict and its variations in time may cause unpredictable consequences (e.g., I/O and CPU speeds of an infrastructure provided as an IaaS service significantly affect response times of hosted applications).

2.3 Security in Cloud Computing

2.3.1 Security of Cloud Applications

In cloud computing, public and private data and operations of an organisation are moved into cloud infrastructure, which is utilised directly as IaaS, as a platform in PaaS, or where provided SW services are running in SaaS service models. In all these cases, the organisation have weaker and only indirect control over the data and operations. This fact significantly affects IT security in the organisation that must implement its security strategy, framework, methods, policies, audits, etc. in cloud to protect various information on its customers, suppliers and other business partners, agreements, accounting, commercial strategies, and know-hows.

The security issues are easier to solve, if the data and operations are stored and performed in a private cloud. In this case, cloud infrastructure is usually located inside the organisation and operated by their employees (i.e., a perimeterised insourcing according to the categorisation from Section 1.1.4). However, most organisations that are not able or willing to maintain their private cloud generally store the data and perform the operations in a public cloud provided by a particular vendor (or vendors). In these cases, the risk of security breaches is quite high and the confidential data may be disclosed, which may cause huge profit loss for the organisation or even legal disputes between the organisation and its customers or business partners.

In 2008, Gartner [53, 54] described seven IT risks of cloud computing in areas such as data segregation and location, privileged user access, service provider viability, regulatory compliance, investigative support, availability, and recovery. Cloud computing should be assessed like any other externally provided service resulting from location independence and the possibility of service provider "subcontracting". According to Gartner, from a security and risk perspective, cloud computing is the least transparent externally sourced service delivery method, storing and processing your data externally in multiple unspecified locations, often sourced from other, unnamed providers, and containing data from multiple customers, where the ability to assess the risk of using a particular service provider comes down to its degree of transparency [53]. Some of the seven cloud-computing IT risks defined by Gartner are not related to IT security and were already discussed in Section 2.2.3, such as a long term *viability* of service dealing with "What would happen to your service if the provider goes broke or is acquired?" [53], the service *availability* where "Organizations should define service-level requirements for any non-trivial IT workload and demand service-level agreements from the provider (internal IT, traditional outsourcer, cloud-computing provider) and ensure that the contract contains penalty clauses when service-level agreements are not met." [53], or *data location* "which should be of concern to anyone needing to meet national privacy regulations" [53]. Other, IT security risk are described in [53, 54] as follows:

- *Privileged user access* should be assessed because, contrary to access control implemented by an organisation into its in-house applications, outsourced de-perimeterised cloud computing services usually bypass all physical, logical, and personnel controls of the organisation.

- *Compliance* of service providers with external audits and security certifications should be required and customers should be provided with information on the specific audits that were evaluated.

- *Data segregation* by application of encryption should be enforced and the correct application of encryption algorithms and decryption key ownership should be audited to prevent unauthorised access to data.

- *Investigative support* should be provided to cloud customers to assist with investigations of inappropriate or illegal activity and electronic discovery. According to [53], cloud services are especially difficult to investigate, because logging and data for multiple customers may be collocated and may also be spread across an ever-changing set of hosts and data centres.

- *Support in reducing risk* to enable customer staff to understand how to safely and reliably use their product, for example, to set policies and monitor them by auditing.

2.3.2 Security Guidance by Cloud Security Alliance (CSA)

The cloud security from a governance, management, and implementation point of view is discussed in [6, 5]. In [5], CSA[33] described fourteen domains of a cloud security analysis focused on cloud architecture (cloud computing architectural framework domain), governing in the cloud (five domains: governance and enterprise risk management; legal issues: contracts and electronic discovery; compliance and audit management; information management and data security; interoperability and portability), and operating in the cloud (eight domains: traditional security, business continuity, and disaster recovery; data centre operations; incident response; application security; encryption and key management; identity, entitlement, and access management; virtualisation; security as a service). To give summaries and recommendations from all these domains is out of scope of this report, therefore, let us focus just on particular parts that are relevant to cloud applications in manufacturing industry.

Risk Assessment

CSA proposed [5] a quick method for evaluating an organisation's tolerance for moving an asset to various cloud computing models. This method consists of the following steps [5]:

1. *Identify the Asset for the Cloud Deployment* that can be either information (data) or transactions/processing (applications/functions/processes), from partial functions all the way up to full applications. For each organisation, it is necessary to determine exactly what its data or function is being considered for the cloud.

2. *Evaluate the Asset* to determine how important the data or function is to the organization by asking questions "How would the organisation be harmed if the security was breached?" for the data or functions.

3. *Map the Asset to Potential Cloud Deployment Models* to determine if the organisation is willing to accept some cloud deployment models: public; private, internal/on-premises; private, external including dedicated or shared infrastructure; community taking into account the hosting location, potential service provider, and identification of other community members; and hybrid with an architectural vision of where components, functions, and data will reside.

4. *Evaluate Potential Cloud Service Models and Providers* with focus on the degree of control the organisation has to implement for risk mitigations in the different software/platform/infrastructure tiers.

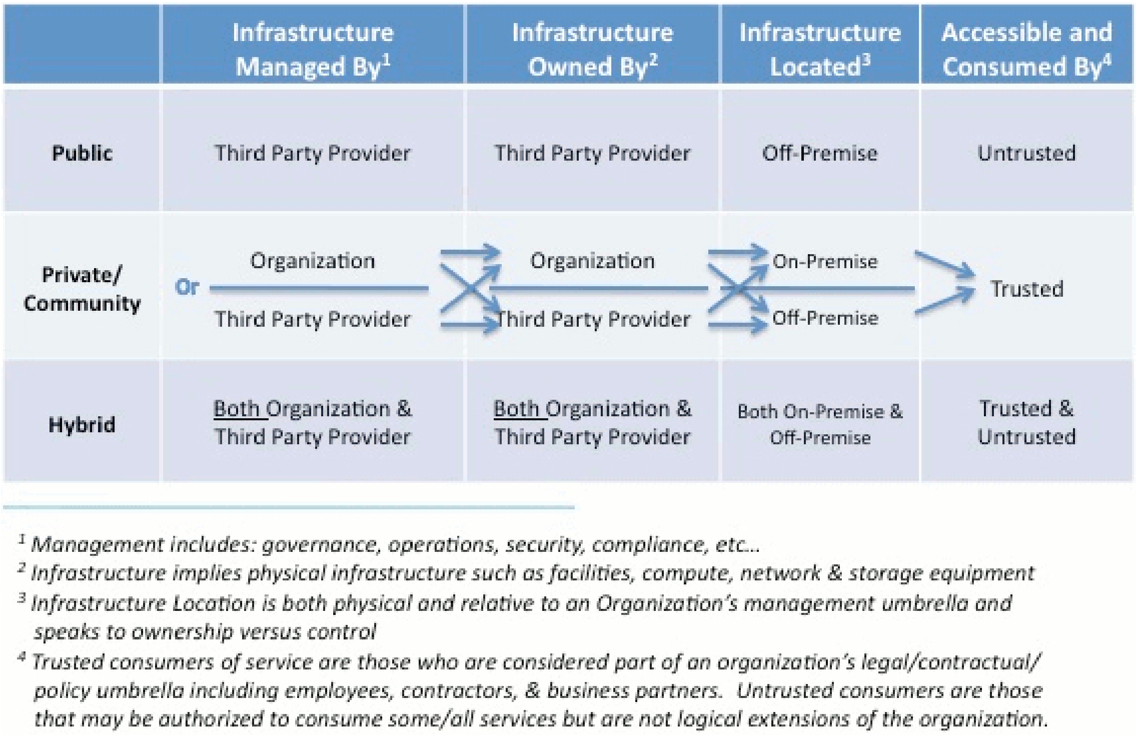
5. *Map Out the Potential Data Flow* between the organization, a cloud service, and any customers/other nodes to understand whether, and how, data can move in and out of the cloud.

Differences in the manageability, ownership, location, and accessibility in the cloud deployments models are described in Figure 2.3.

Security Control and Compliance Model

As the cloud computing services are provided and organised hierarchically in the cloud model at various layers in individual IaaS/PaaS/SaaS service models (see Section 1.1.2),

[33] `https://cloudsecurityalliance.org/`



	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Or Organization Third Party Provider	Organization Third Party Provider	On-Premise Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

[1] Management includes: governance, operations, security, compliance, etc...

[2] Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment

[3] Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control

[4] Trusted consumers of service are those who are considered part of an organization's legal/contractual/ policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

Figure 2.3: Cloud computing deployment models and manageability, ownership, location, and accessibility (adopted from [5]).

different control measures and compliance procedures can be assigned to these levels as depicted in Figure 2.4. While the security control model applies mainly technical and organisational measures set up for a particular organisation, the compliance model is often given by legal documents, certification procedures, or security standards. For example, the compliance model can be given by Payment Card Industry (PCI)[34] rules for e-commerce worldwide, or by Health Insurance Portability and Accountability Act (HIPAA)[35] privacy and security rules, Gramm-Leach-Bliley Act (GLBA)[36] for financial institutions, or Sarbanes-Oxley Act (SOX)[37] to deter fraud and increase corporate accountability, in the United States of America.

Information Management and Data Security

To implement data security in the cloud, CSA [5] recommends Data Security Lifecycle by Securosis[38] which includes six phases from data creation to its destruction. During those phases, data goes through a cloud environment and are operated: accessed, processed, and stored. It is necessary to identify and control these operations in the individual phases of the data security life-cycle including actors of these operations (who can perform the operations and is allowed to do so) and locations (where the operations can be performed and are allowed). The operations that can be performed but are not allowed in particular cases must be restricted by security policies.

[34] `https://www.pcisecuritystandards.org/`

[35] `https://www.hhs.gov/hipaa/`

[36] `https://www.ftc.gov/consumer-protection/gramm-leach-bliley-act`

[37] `http://csrc.nist.gov/groups/SNS/rbac/sarbanes_oxley.html`

[38] `https://www.securosis.com/blog/data-security-lifecycle-2.0`

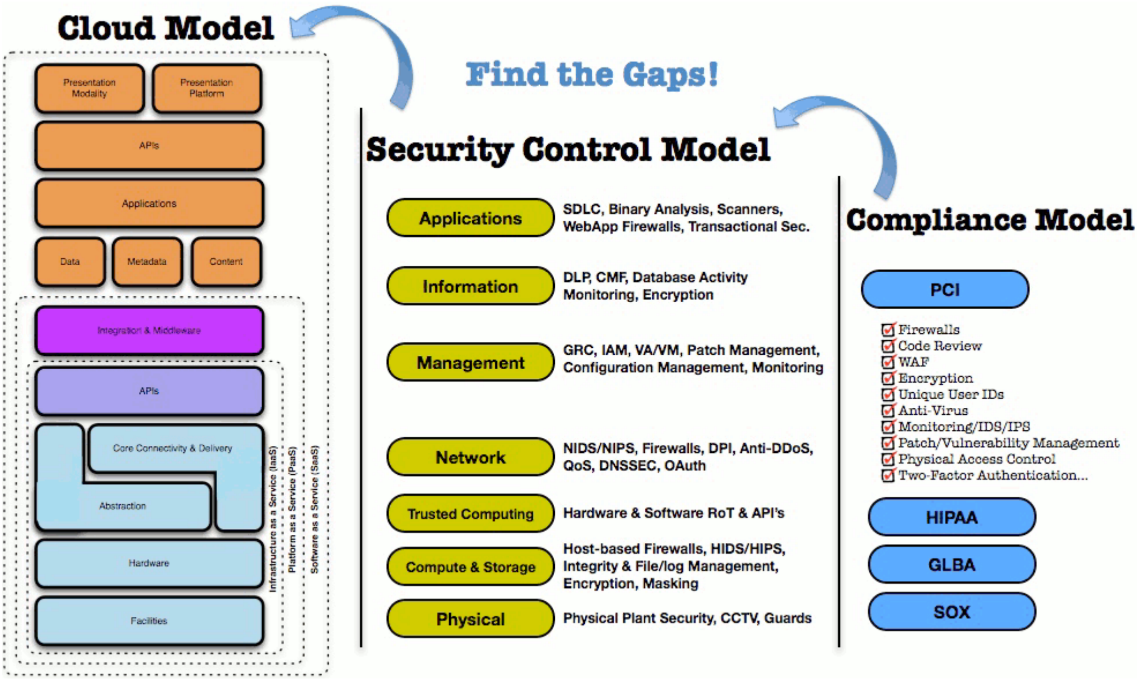

Cloud Model
Presentation Modality
Presentation Platform
APIs
Applications
Data
Metadata
Content
Integration & Middleware
APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Find the Gaps!
Security Control Model
Applications
SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information
DLP, CMF, Database Activity Monitoring, Encryption
Management
GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network
NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing
Hardware & Software RoT & API's
Compute & Storage
Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical
Physical Plant Security, CCTV, Guards
Compliance Model
PCI
☑ Firewalls
☑ Code Review
☑ WAF
☑ Encryption
☑ Unique User IDs
☑ Anti-Virus
☑ Monitoring/IDS/IPS
☑ Patch/Vulnerability Management
☑ Physical Access Control
☑ Two-Factor Authentication...
HIPAA
GLBA
SOX

Figure 2.4: The cloud model mapping to security control & compliance (adopted from [5]).

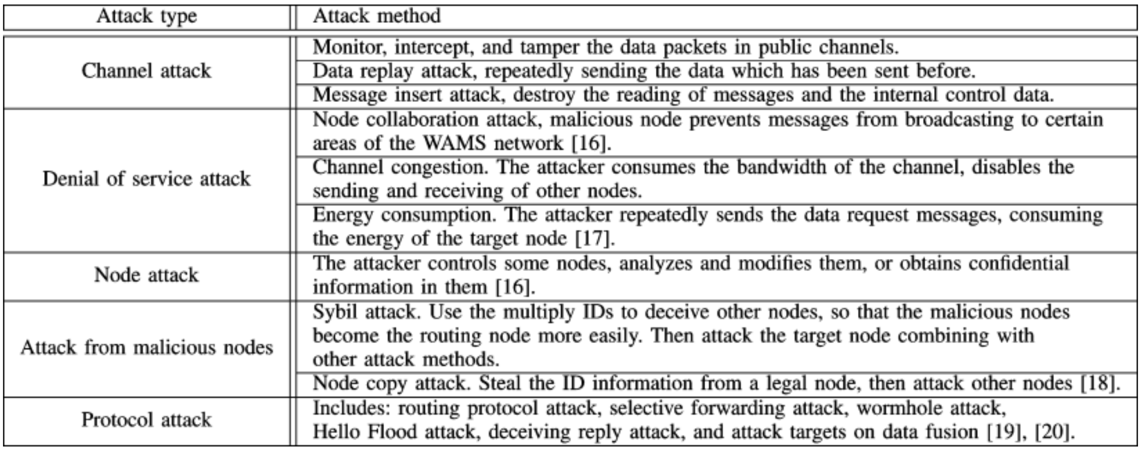
According to CSA [5], data privacy protection on the boundary and within the cloud can be ensured by client/application (document) encryption, link/network encryption (e.g., Secure Sockets Layer (SSL) or VPNs), and proxy-based encryption (by a proxy appliance or server, which encrypts data before sending further on the network). Such the encryption can be applied in all service models (IaaS/PaaS/SaaS) by various technical means as described in [5]. Moreover, there are another recommendations on data loss prevention (DLP), database and file activity monitoring (DAM/FAM), digital rights management (DRM) and others.

2.3.3 Security in Edge/Fog Cloud and Cloud Manufacturing

In the case of edge or fog computing, which is the concept typically utilised in CMfg to connect and integrate various devices into the cloud (such as production machines, robots, wireless sensor network gateways, etc.), another security aspect need to be considered. As the CMfg usually integrate many small devices providing their service into the cloud, these devices are interconnected via a local, usually wireless, network infrastructure. Attacks targeting a manufacturing cloud may focus on this infrastructure to harm the cloud services.

While wired network infrastructure can be physically protected quite easily, the protection of wireless network infrastructure in much more difficult. At low levels, the wireless networks usually utilise proprietary communication technologies, proprietary extensions of open protocols, or proprietary firmware and drivers of standardised technologies, such as in the case of various implementations of ZigBee/IEEE 802.15.4 standard[39]. These technologies and protocols implement low-level layers of a network stack (e.g., IEEE 802.15.4 deals with physical and medium-access-control layers and ZigBee covers network and application layers). Upon these layers, high-level communication buses are built that implement the

[39] http://www.zigbee.org/



Attack type	Attack method
Channel attack	Monitor, intercept, and tamper the data packets in public channels.
	Data replay attack, repeatedly sending the data which has been sent before.
	Message insert attack, destroy the reading of messages and the internal control data.
Denial of service attack	Node collaboration attack, malicious node prevents messages from broadcasting to certain areas of the WAMS network [16].
	Channel congestion. The attacker consumes the bandwidth of the channel, disables the sending and receiving of other nodes.
	Energy consumption. The attacker repeatedly sends the data request messages, consuming the energy of the target node [17].
Node attack	The attacker controls some nodes, analyzes and modifies them, or obtains confidential information in them [16].
Attack from malicious nodes	Sybil attack. Use the multiply IDs to deceive other nodes, so that the malicious nodes become the routing node more easily. Then attack the target node combining with other attack methods.
	Node copy attack. Steal the ID information from a legal node, then attack other nodes [18].
Protocol attack	Includes: routing protocol attack, selective forwarding attack, wormhole attack, Hello Flood attack, deceiving reply attack, and attack targets on data fusion [19], [20].

Figure 2.5: Major security threats in a WAMS (adopted from [55]; for references in the figure, see the source).

CMfg as described in Section 2.1.2. Although the high-level communication buses usually have a very good and customisable security, such security measures cannot prevent all impacts of security breaches at the low-level layers.

For example, Figure 2.5 describes security threats from [55] encountered in a wide-area monitoring system (WAMS) implementation as a smart grid, which is very similar to the CMfg concept[40].

Some of these attacks can be prevented at the high-level communication buses, for example, by applying a strong encryption and encapsulating the transferred data into encrypted containers. However, this approach has at least two drawbacks: (1) it cannot improve security of operations that stay at lower levels (for example, packet routing) and (2) the encryption and decryption which must be done at edge node low-power devices will consume large amounts of processor time, operating memory, and certainly also electric energy, which may be critical for wireless devices. These problems are discussed in [55] for lower levels and in [56] for higher levels. The second referred publication also describes types of the potential attacks against WAMS smart grid as follows [56]:

- *Loss of confidentiality* by (i) eavesdropping and analysing the wireless transmission; (ii) node capturing and replication.

- *Loss of authenticity* by (i) message modification and insertion; message replay; (ii) node capturing and replication; (iii) Sybil attack in which a small number of malicious nodes forge a large number of fake identifications to cheat or disrupt the message routing.

- *Loss of integrity* by message modification.

- *Loss of availability* by (i) message blocking by collaboration of the malicious nodes, wireless channel jamming; (ii) fake data request to the sensors that cause unnecessary energy consumption.

Before the security issues above will be solved at all levels of the CMfg communication stack by research community and adopted by vendors, it is strongly recommended to stay with conservative methods of networking in the cloud, e.g., to prefer wired networking

[40] for a grid and cloud computing comparison, see [2]

over wireless networking and to keep critical data and operations in highly secured private clouds, rather than building hybrid clouds or on public cloud services. Otherwise, successful attacks on devices connected into a manufacturing cloud may cause not only a data loss or a data breach, but also the attacked devices, such as production machines or robots, may physically operate in a destructive way and cause a large property loss.

3 Overview and Comparison of Cloud Computing Services

In the previous chapters, theoretical foundations of cloud computing have been presented including their practical aspects for manufacturing industry. We described several service models and deployments, their categorisations, architectures, trends, etc. Along this description, several cloud computing solutions have been mentioned provided by both particular vendors and open community. In this chapter, available cloud computing services for manufacturing industry will be listed, categorised, and compared according to their purpose and other criteria. Moreover, three selected cloud computing services dealing suitable for cloud manufacturing (CMfg) will be analysed in more details to evaluate how they are fulfilling the principles of CMfg and addressing possible opportunities and threats.

Comparison criteria (CC) will be used in the comparative analysis described above. The goal of these criteria is not to select the best cloud computing solution but to establish common ground for the objective comparison which is necessary, as the individual solutions target different needs. The evaluation of the cloud computing solutions should be always done within the context of their generic application domain, or for a particular target user in mind if possible. The CC are the following:

CC1 *Characteristic service model* (IaaS/PaaS/SaaS) – The cloud computing solutions usually offer various services at different service levels, i.e., Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). However, only one of these models is often characteristic for main services that are significantly contributing to business or production processes in a customer's organisation. There can be also other cloud services with different service models acting as auxiliary for the main services or specialised for particular use-cases, e.g., Robot as a Service (RaaS). However, during the comparison, only characteristic service models will be identified.

CC2 *Cloud architecture* (static/edge/fog) – Cloud computing infrastructure and services are organised in layers from low-level IaaS to high-level SaaS services and the corresponding infrastructure. In common well-established cloud computing solutions with a static architecture, the cloud infrastructure is distributed and virtualised to provide users with uniform services at all geographical locations. Contrary to that in the case of edge/fog cloud computing, cloud architecture is composed from various simple devices, such as programmable logic controller (PLC) or virtual robot controller (VRC), as well as big distributed platforms (as in the previous case) that both provide services of various service models, e.g., Data as a Service (DaaS), Manufacturing as a Service (MaaS), etc. It is useful to distinguish such different architectures. Moreover, for the purpose of this comparison, we will distinguish between the edge cloud computing where edge devices just serve data to the cloud or enable to control connected machines (e.g., stand-alone DaaS services) for smart manufacturing, see Section 2.1.1) and the fog computing where the edge devices both provide their services to the rest of the cloud and also utilise other services in the cloud for their own purposes (i.e., well-integrated CMfg, see Section 2.1.2).

CC3 *Cloud Cube Model (CCM) classification* (I/E, P/O, Per/D-p, and In/Out) – To evaluate deployment aspects of individual cloud computing solutions, the CCM by Jericho Forum will be utilised (see Section 1.1.4). By this model, each cloud computing solution will be assigned with one of each: Internal/External (I/E) to define the physical location of the data in the cloud; Proprietary/Open (P/O) to describe the state of ownership of the cloud infrastructure and services; Perimeterised/De-perimeterised (Per/D-p) to identify how the cloud infrastructure is controlling data and functions in the cloud relative to inside/outside boundaries of a customer's organisation; Insourced/Outsourced (In/Out) to decide who is managing delivery of the cloud services utilised by a customer's organisation.

CC4 *Data analytics* (none/predefined/custom/Big data) – Cloud computing services manage and generate a lot of data that represents values of metrics of business or production processes, sensor data from monitoring, data accessible by DaaS, data stored in cloud storage services, etc. A large amount of runtime generated data is also typical for CMfg. Analysis of such data is a complex task which should be supported by the cloud. Therefore, the cloud services may offer predefined analyses for well-known key performance indicators (KPIs) or let customers to implement their own custom analytics. Moreover, there is need for Big data processing and analytics, as it was described in Section 1.2.3.

CC5 *Security* (access control, encryption, etc.) – Security in cloud computing is a big issue and must be enforced by both cloud providers and their customers as described in Section 2.3. This is usually done by strict access control with accounting and storage and communication encryption. As described before, there are multiple ways hot to implement these security features. However, there exists another security features, such as services for identity management, single sign-on services, or distributed trust networks, that make the comparison of cloud computing solutions according to this criteria more difficult.

CC6 *Opportunities* and *Threats* (see the list in Section 2.2) – In the previous sections of this report, several opportunities and threats of cloud computing (and manufacturing cloud) have been identified. While many of them are successfully addressed by the cloud computing solutions in the comparison below, others represent possible profits or looses that need to be considered.

3.1 Cloud Computing Services for Manufacturing Industry

Based on the state-of-the-art analysis in the previous chapters (especially on Section 2.1), the most promising for automotive/electronics manufacturing industry is the application of cloud computing for smart manufacturing (to monitor, control, and optimize business, management, and supporting processes) and CMfg (to monitor, control, and optimize manufacturing processes and asset utilisation in the manufacturing; see Sections 2.1.1 and 2.1.2, respectively). Cloud solutions available on the market today for manufacturing industry focus mostly on the smart manufacturing, not the CMfg, utilising the concept of Internet of Things (IoT). Yet, their custom deployments with thorough applications of CMfg principles in the cases of particular manufacturing organisations can move these solutions towards the CMfg.

This section provides a brief overview of several currently available cloud solutions that might be suitable for manufacturing industry as described in the paragraph above[1]. Another three most promising of these solutions are described in details in Section 3.2. Overall results of the comparison are shown in Table 3.1.

3.1.1 AWS IoT

Amazon Web Services (AWS) IoT is a managed cloud platform that lets connected devices easily and securely interact with cloud applications and other devices. AWS IoT can support billions of devices and trillions of messages, and can process and route those messages to AWS endpoints and to other devices reliably and securely. AWS IoT makes it easy to use AWS services like AWS Lambda, Amazon Kinesis[2], Amazon S3[3], Amazon DynamoDB[4], etc. to build IoT applications that gather, process, analyse, and act on data generated by connected devices, without having to manage any infrastructure. [58]

According to [59], AWS IoT provides secure, bi-directional communication between Internet-connected things (such as sensors, actuators, embedded devices, or smart appliances) and the AWS cloud to collect telemetry data from multiple devices and store and analyse the data. AWS IoT systems can be built from several components: device gateway (to enable devices to securely and efficiently communicate), message broker (for applications to publish and receive messages from each other by Message Queue Telemetry Transport (MQTT) protocol), rules engine (to create message processing and integration rule), security and identity service (to provide shared responsibility for security), thing/device registry (to organize the resources associated with each thing/device, such as for certificates and MQTT client identifications), thing/device shadow (to store and retrieve current state information for a thing/device), and thing shadows service (to provide persistent representations of things/devices in the cloud).

AWS IoT, if taken together with the rest of AWS cloud services, is PaaS for edge cloud computing, which can be deployed as external, proprietary, de-perimeterised, and insourced cloud solution according to the CCM by Jericho Forum (see Section 1.1.4), with highly custom/Big data analytics (provided by particular AWS data-analytics services), with encrypted communication, authentication and access control with identity management (by the security and identity service). It is good in addressing opportunities O1, O3, O5, O7, and O9 and threats T3 and T6 according to Section 2.2, however, threats T1, T4, and T5 are not addressed well, mainly due to strict (vendor) dependency on Amazon technologies.

From the point of view of CMfg, AWS IoT is not suitable as it is missing industrial application programming interfaces (APIs) and the ability to deploy as an internal perimeterised hybrid or private cloud, despite of the existence of Amazon Virtual Private Cloud which is not satisfactory (it is not a “private” cloud, but an external perimeterised hybrid cloud according to Section 1.1.3).

3.1.2 IBM BlueMix / Watson IoT Platform

IBM BlueMix is a cloud computing solution from IBM that offers a large amount of various cloud services[5]. It is based on Cloud Foundry open technology[6]. According to [60],

[1] A technical comparison of some of the discussed cloud solutions can be found in [57].

[2] `https://aws.amazon.com/kinesis/`

[3] `https://aws.amazon.com/s3/`

[4] `https://aws.amazon.com/dynamodb/`

[5] see `https://console.bluemix.net/catalog/`

[6] `https://www.cloudfoundry.org/`

Service Name	**CC1 Model**	**CC2 Arch.**	**CC3 CCM**	**CC4 Analytics**	**CC5 Security**	**CC6 Opport.**	**CC6 Threats**
AWS IoT (Sec 3.1.1)	PaaS	edge	E, P, D-p, In	custom / Big data	encrypted comm., auth., access ctrl., identity mgmt.	$O1+$, $O3+$, $O5+$, $O7+$, $O9+$	$T3+$, $T6+$; $T1-$, $T4-$, $T5-$
IBM BlueMix, Watson IoT (Sec 3.1.2)	PaaS	edge	E, O/P, Per/D-p, In	custom / Big data	encrypted comm., auth., access ctrl., identity mgmt.	$O1+$, $O2+$, $O3+$, $O4+$, $O5+$, $O6+$, $O7+$, $O9+$	$T1+$, $T3+$, $T4+$, $T5+$; $T6-$
Microsoft Azure IoT (Sec 3.1.3)	PaaS	edge	E, O/P, D-p, In	custom	encrypted comm.	$O3+$, $O5+$, $O8+$, $O9+$; $O1-$, $O2-$, $O7-$	$T5+$, $T6+$; $T1-$, $T3-$, $T4-$
Google Cloud IoT (Sec 3.1.4)	PaaS	edge	E, P, De-p, In/Out	Big data	encrypted comm.	$O1+$, $O3+$, $O8+$, $O9+$; $O7$; $O2-$, $O4-$	$T3+$, $T6+$; $T1-$, $T4-$, $T5-$
SAP Cloud Platform for IoT (Sec 3.1.5)	PaaS	edge	E, P, De-p, In	custom / Big data	encrypted comm., auth.	$O4+$, $O5+$, $O8+$, $O9+$; $O1-$, $O3-$	$T3+$; $T1-$, $T4-$, $T5-$, $T6-$
Mnubo (Sec 3.1.6)	SaaS	N/A	E, P, De-p, Out	custom	encrypted comm., auth.	$O5+$, $O9+$	$T1+$; $T3-$, $T4-$
PTC Thing-Worx (Sec 3.2.1)	PaaS	edge	E/I, P, De-p, In/Out	predefined / custom	encrypted comm., auth., access ctrl.	$O1+$, $O2+$, $O3+$, $O5+$, $O7+$, $O9+$	$T4+$, $T6+$; $T3$; $T1-$, $T5-$
Siemens Mind-Sphere (Sec 3.2.2)	SaaS (PaaS)	edge	E/I, P, De-p, In	predefined / Big data	encrypted comm., encrypted storage, auth., access ctrl.	$O1+$, $O3+$, $O5+$, $O9+$; $O2-$	$T5+$, $T6+$; $T4$, $T3$; $T1-$
GE Predix (Sec 3.2.3)	PaaS	edge	I, P, De-p, In	custom	encrypted comm., auth., access ctrl., identity mgmt.	$O1+$, $O2+$, $O3+$, $O5+$, $O9+$; $O7-$, $O8-$	$T1+$, $T3+$, $T4+$, $T6+$; $T5-$

Table 3.1: The comparison of cloud computing services for manufacturing industry. For CC, see Chapter 3. Plus/minus (+/−) signs in CC6 columns mark supported/missed opportunities and threats (see Section 2.2).

in Watson IoT Platform, a thing/device is connected into BlueMix cloud directly or via a gateway by a messaging protocol based on open MQTT or proprietary Hypertext Transfer Protocol (HTTP) Messaging API. Data provided by the device are processed by services in the cloud and the services' functions and resulting data are accessible via Representational State Transfer (REST) interface. In the cloud, there are BlueMix services for device management, user and user role management and access control (for users, roles, applications, and devices), real-time data analytics including (partial) analytics on edge devices (on IoT gateways with Watson IoT Edge Analytics Agent), visualisations, and others.

From the point of view of the manufacturing industry, BlueMix provides several cloud services or whole service frameworks such as IBM Watson IoT Platform[7], or its specialisations for automotive or electronics industry[8]. There are several such ready-to-use services for various industrial applications of IoT in smart manufacturing with cloud computing or CMfg (see Sections 2.1.1 and 2.1.2, respectively). However, devices connected to the cloud are primarily integrated as data sources, not as clients of the cloud that would utilise it as in fog computing according to Section 1.2.1.

Watson IoT Platform with IBM BlueMix can be categorised as PaaS cloud for edge computing, which can be deployed as external, open IoT with proprietary cloud, perimeterised or de-perimeterised, and insourced cloud solution according to the CCM by Jericho Forum (see Section 1.1.4). The perimiterisation depends on architecture, which can be managed by vendor for public cloud or by customer for private cloud solutions. In the last case, BlueMix Local [61] creates an inception virtual machine running on the customer's information technology (IT) infrastructure, which is working locally and relaying to the public vendor-managed cloud just in special cases (such as for IT/service operation management). This may significantly improve security of the cloud solution.

To continue with the categorisation, BlueMix cloud services provide highly custom/Big data analytics, with encrypted IoT-to-cloud communication and authentication and access control with identity management. This cloud solution is good in addressing opportunities O1–O6 (due to openness and architectural flexibility), O7 (there is the IoT for Automotive service mentioned above), and O9 (good cloud services for data analytics and visualisation), according to Section 2.2. Concerning the threats in the same section, T1 is good but not perfect (most of IBM BlueMix and Watson IoT Platform is open-source) and also T3, T4, and T5 are addressed well (due to the flexible architecture). Yet, there are still another threats, such as T6, that need to be addressed better.

3.1.3 Microsoft Azure IoT Suite

In 2015, Microsoft announced Azure IoT Suite, a cloud computing solution based on Azure Cloud Platform[9]. Applications developed in Azure IoT Suite can utilise Azure IoT Hub or Azure IoT Edge for asset device management and deployment, or Azure Machine Learning[10], Stream Analytics[11] and Time Series Insight[12] for advanced data analytics.

According to [62], Azure IoT Hub is a bridge for secure, reliable, two-way communication between IoT devices and the cloud over open protocols MQTT, REST, and Advanced Message Queuing Protocol over TLS/SSL (AMQPS). It allows the devices to establish

[7] `https://console.bluemix.net/catalog/services/internet-of-things-platform`

[8] see `https://console.bluemix.net/catalog/services/iot-for-automotive/` and `https://console.bluemix.net/catalog/services/iot-for-electronics/`, respectively

[9] see `https://www.microsoft.com/en-us/internet-of-things/azure-iot-suite`

[10] `https://azure.microsoft.com/services/machine-learning/`

[11] `https://azure.microsoft.com/services/stream-analytics/`

[12] `https://azure.microsoft.com/services/time-series-insights/`

secure connections and send or receive messages to or from the cloud, e.g., to store, analyse and act on that data in real time. Azure IoT Edge[13] allows to read data of assets via industry standard communication protocols such as OPC Unified Architecture (OPC-UA), Modbus and MQTT [63] and to pre-process the data in an on-premises gateway with Azure IoT Edge software (SW) on Linux or Windows operating system. The pre-processing is performed in the gateway edge device before it sends the data to the cloud so that only the most important information is uploaded. Moreover, the device can operate reliably and securely even when there is intermittent cloud connectivity, so once reconnected, it automatically synchronizes its latest state and continues to function seamlessly [64]. In combination with Azure Stream Analytics, the data can be in the pre-processing not only filtered down, but also aggregated on a time window, or using a user-defined function, or processed directly on the device without passing to the cloud [63].

Microsoft announced Azure IoT Suite is PaaS for edge cloud computing, which can be deployed as external, open/proprietary (Azure IoT Edge is open, the cloud is proprietary based on Microsoft technologies), de-perimeterised, and insourced cloud solution according to the CCM by Jericho Forum (see Section 1.1.4), with custom analytics (provided by Azure Stream Analytics service for the edge cloud) and encrypted communication. The suite does not focus on authentication and access control or identity management, however, these are partially covered by Azure Cloud Platform. It is good in addressing opportunities O3, O5, O8, and O9 and threats T5 and T6 according to Section 2.2. Opportunities O1, O2, and O7 and threats T1, T3, and T4 are not addressed well, mainly due to strict (vendor) dependency on Microsoft technologies. Contrary to the most of other cloud solutions described in this report, Azure IoT Edge partially solves well threat T5 by the processing on edge devices even with intermittent cloud connectivity as mentioned above.

3.1.4 Google Cloud IoT

Google Cloud IoT is a set of fully managed and integrated cloud computing services that allows to easily and securely connect, manage, and ingest IoT data from globally dispersed devices at a large scale, process and analyse/visualize that data in real time, and implement operational changes and take actions as needed. Device data captured by Cloud IoT Core gets published to Cloud Pub/Sub for downstream analytics. Ad-hoc analyses can be done using Google BigQuery[14], advanced analytics and machine learning with Cloud Machine Learning Engine[15], or visualisation of IoT data results with rich reports and dashboards in Google Data Studio[16]. [65]

According to [66], Google Cloud IoT is managing, storing, or analysing device metadata (such as identifier, model, or hardware (HW) serial number), state information, telemetry (data usually collected through sensors and available through channels in the cloud), and operational information (such as central processing unit (CPU) operating temperature and battery state). The devices can be connected into the cloud directly[17], or through a gateway's HW interfaces as sensors. Devices might handle and process the sensor data before sending them into the cloud, e.g., to convert, package, validate, sort, enhance, summarise, or combine the data from one or more sensors and time spans. After that, the data is submitted via an encrypted connection to the cloud by Google Cloud Pub/Sub[18]

[13] `https://github.com/azure/iot-edge`

[14] `https://cloud.google.com/bigquery/`

[15] `https://cloud.google.com/ml-engine/`

[16] `https://www.google.com/analytics/data-studio/`

[17] For HW and SW partners of Google Cloud IoT, see `https://cloud.google.com/iot/partners/`.

[18] `https://cloud.google.com/pubsub/`

globally durable message ingestion service (for any data), or by Stackdriver Monitoring or Logging[19] (for operational data and events). In the cloud, data can be processed in pipelines (transformed, aggregated, enriched, and moved into final storage locations) by Cloud Functions[20] or Cloud Dataflow[21] services. The processing pipelines may include storing data in Firebase platform[22], Cloud Storage Nearline[23], or Cloud Bigtable[24], or data analytics in Cloud Datalab[25], BigQuery, and others described in the paragraph above.

Contrary to the other vendors discussed in this document, Google Cloud IoT provides just a basic PaaS cloud solution without any specialisation to particular application area, such as to manufacturing industry. Although the existence of experimental applications of Google Cloud IoT for selected areas, such as a connected vehicle platform in [67], practical applications are supposed to be provided by HW and SW partners, such as Mnubo (see Section 3.1.6). Google Cloud IoT implements edge computing (however, not such good as Azure IoT Edge in Section 3.1.3) and can be deployed as external, proprietary, de-perimeterised, and insourced/outsourced (depends on the particular implementation) cloud solution according to the CCM by Jericho Forum (see Section 1.1.4). Custom as well as Big data analytics is supported (see the paragraph above). There is end-to-end security (encrypted communication), however, advanced authentication, access control, and identity management should be provided explicitly, e.g., by integration of Google Cloud Identity & Access Management service[26] or other third-party services.

Google Cloud IoT is good in addressing opportunities O1 (low-cost commodity HW), O3, O5, O8, and O9 and threats T3 (open data) and T6 according to Section 2.2. Opportunities O2 (proprietary) and O4 (very variable architecture) and threats T1, T4, and T5 (processing mostly in the cloud) are not addressed well. In the case of opportunity O7, although there is a connected vehicle platform [67], it is a rather experimental proof-of-concept use case than a ready-to-use practical solution.

3.1.5 SAP Cloud Platform for IoT

SAP Cloud Platform for IoT is a platform based on SAP HANA Cloud Platform which can help quickly develop, deploy, and manage real-time IoT and machine-to-machine (M2M) applications. From SAP HANA Cloud Platform based on SAP HANA Database, the IoT platform inherit the ability of real-time in-memory stream processing and support for text analysis, geo-spatial and series data, and location services with a graph engine. [68]

According to [69], an IoT device can register itself into SAP Cloud Platform by Remote Device Management Service. After the registration, the device sends messages to or receives messages from the cloud by communication with Message Management Service. The messages sent into the cloud can be directly processed by third-party services (such as by a document service) and are stored into SAP HANA[27], or into relational databases SAP MaxDB[28] and SAP ASE[29], where the messages can be retrieved by IoT application running in the cloud. The applications can also send messages to and receive messages from the

[19] https://cloud.google.com/stackdriver/

[20] https://cloud.google.com/functions/

[21] https://cloud.google.com/dataflow/

[22] https://firebase.google.com/

[23] https://cloud.google.com/storage-nearline/

[24] https://cloud.google.com/bigtable/

[25] https://cloud.google.com/datalab/

[26] https://cloud.google.com/iam/

[27] https://www.sap.com/products/hana.html

[28] http://maxdb.sap.com/

[29] https://www.sap.com/products/sybase-ase.html

devices by direct communication with Message Management Service. Both the devices and the applications can communicate with Message Management Service via HTTP or Hypertext Transfer Protocol over Transport Layer Security (HTTPS), WebSocket, and MQTT protocols. The communication is encrypted by Transport Layer Security (TLS) and devices are authenticated by OAuth or client certificates, while the applications are authenticated by username and password, or by OAuth. For secure device registration management by means of IoT Service Cockpit application, Security Assertion Markup Language (SAML) is utilised.

SAP Cloud Platform for IoT is PaaS for edge cloud computing, which can be deployed in public cloud as external, proprietary, de-perimeterised, and insourced cloud solution according to the CCM by Jericho Forum (see Section 1.1.4). Despite of the categorisation as the edge cloud computing, device data processing is done solely in the cloud, not on the edge devices that just send (or receive) the data (contrary to the edge cloud solutions of other vendors). The data received from IoT device are can be stored into SAP HANA for Big data analyses or analysed by custom services (directly or by storing in and querying relational databases). Security is ensured by encrypted communication and authentication. Possible access control and identity management should be implemented in external OAuth service.

The platform is good in addressing opportunities O4 (predefined architecture), O5, O8, and O9 and threat T3 (open databases) according to Section 2.2, however, the rest of the opportunities and threats are not addressed well due to proprietary technologies, simple security, and the predefined (fixed) architecture with just elementary cloud services in SAP Cloud Platform for IoT. Although the existence of SAP HANA Cloud Platform services and use-case applications for various application domains, they have poor public documentation and no or just simple integration with SAP Cloud Platform for IoT (no real edge/fog cloud computing).

3.1.6 Mnubo: Analytics for Industrial Equipment

Mnubo is an SaaS solution providing a comprehensive Big Data platform catering to IoT via three solutions: mnubo SmartObjects cloud, mnulabs and mnubo SmartObjects analytics. Mnubo facilitates business logic modelling and Big data analytics. It is the premier platform for IoT developers to build, deploy and manage real world business rules and applications using machine data and derive advanced analytics and business insights for further innovation. [70]

According to [71], mnubo SmartObjects is IoT cloud for receiving, processing, and analytics on events (data) from objects (assets) and their owners (customers). Objects are assets such as IoT devices of partner IoT platforms[30] (e.g., Google Cloud IoT enabled devices). An event consists of an event type (a source of the change), a timestamp and one or more optional numerical or non-numerical time-series values. By the event, SmartObjects cloud is notified that an object change has taken place. The objects send events via REST API to a private server connected to a public cloud in a hybrid cloud deployment, or directly to the public cloud. In both cases, the public cloud is utilised for data analytics. The communication is encrypted by HTTPS and each event is secured by a client access token which the client device gets from the cloud after successful registration by the client's identifier and secret. SmartObjects public cloud provides cloud services for Activity/Inactivity Analytics, Enrichment (by geographical and weather context of the device), Life Cycle Analytics, Scoring (by owners), Session Analytics (between a specific start and

[30] http://mnubo.com/partners/

stop event), Time-series Predictions, and artificial intelligence (AI)/machine learning (ML) Workbench (for machine learning and predictions).

As mentioned above, mnubo is a SaaS solution with public or hybrid cloud deployment. It utilises underlying PaaS of partner IoT platforms, such as Google Cloud IoT. According to the CCM by Jericho Forum (see Section 1.1.4), mnubo can be categorised as external, proprietary, de-perimeterised, and outsourced cloud solution. For security, mnubo encrypts communication and requires authentication of the devices by access tokens or secret passwords. Currently, there is no custom identity or access control management.

Mnubo is good in addressing opportunities O5 and O9, and threat T1 (support for various PaaS) according to Section 2.2. Threats T3 and T4 are not addressed well as the SaaS solution is proprietary and closed (except for client libraries that are open-source). Addressing of other opportunities and threats depends on utilised underlying PaaS.

3.2 Comparison of Selected Cloud Computing Services

After a consultation with a target audience of this report, three cloud computing services have been selected for a thorough analysis and comparison – ThingWorx by PTC; MindSphere by Siemens; and Predix by General Electric (GE). All of these platforms support industrial edge computing by the IoT concept and can provide services at various degrees of complexity, from a simple integration of IoT in the case of ThingWorx to PaaS analytics in the case of Predix.

3.2.1 PTC ThingWorx

In May 2017, PTC[31] has already released the version 8 of platform for IoT and augmented reality (AR) called ThingWorx[32]. ThingWorx is said to be an open PaaS devoted for IoT and AR built over ThingWorx Foundation, which enables to interconnect various devices in IoT (especially their sensors) and deliver their data to whatever a customer may need. Together with a set of other applications and utilities, it provides a way for edge computing together with industrial real-time operational intelligence to make more proactive and faster decisions. Moreover, tools and tool-chains are prepared to develop user specific applications for AR and IoT in general. Namely, the ThingWorx Foundation is surrounded with ThingWorx Analytics, ThingWorx Utilities, ThingWorx Studio, and ThingWorx Industrial Connectivity[33]. To extend the IoT technology stack in ThingWorx to M2M applications, Axeda Corporation was acquired by PTC in 2014 and Axeda Machine Cloud[34] was integrated into PTC ThingWorx.

ThingWorx may be running either on servers hosted by PTC, or it can be deployed on AWS IoT[35] [58], and finally Microsoft Azure IoT Hub[36] is also supported. Moreover, deployment on user cloud machines is probably possible as well if assuring and providing necessary features. After deployment, the ThingWorx PaaS provides ready-to-use environment, where various elements may be interconnected and deployed, such as a user specific data store (various database management systems are supported, including SAP), industrial analytical applications, AR applications for end-users, etc.

[31] https://www.ptc.com/

[32] https://www.thingworx.com/

[33] see https://www.thingworx.com/platforms/thingworx-foundation/ and therein referenced items

[34] https://www.ptc.com/axeda

[35] https://aws.amazon.com/iot/

[36] https://azure.microsoft.com/en-us/services/iot-hub/

Characteristic Service Model: PaaS

Users obtain a ready-to-use platform with numerous extensions and development tools to build their own applications. Thus, users can communicate with numerous devices in a uniform way to deliver analytical information about usage/status of the devices in IoT and, therefore, prediction of possible failure may be detected in advance. Other typical usage is creation of AR applications supporting end-users (e.g., showing an end-user how to fill in cooling liquid in her/his car) or even service-engineers (e.g., how to replace broken pump in a car).

All the tools and ready-to-use utilities are built around ThingWorx Foundation. ThingWorx Studio allows application development, where AR applications are targeted to iOS, Android, and HoloLens[37].

Cloud Architecture: Edge

The architecture of ThingWorx is quite simple. It connects IoT devices with target applications consuming data provided by the IoT devices. Thus, there are basically three elements present in the chain: a source IoT device, ThingWorx PaaS, and a target application of any kind.

The ThingWorx Foundation defines these three elements the following way.

1. The ThingWorx Foundation Core includes Application Enablement Platform (AEP) and Platform Services.
2. The ThingWorx Foundation Connection Services include Connection Servers, Device/Cloud Adapters, and Tunneling Servers.
3. The ThingWorx Foundation Edge includes Edge MicroServer and Edge "Always On" software development kit (SDK).

Around ThingWorx Foundation, there are four additional SW applications/tool-sets that provide ways to build applications, connect SW devices, perform analytical operations, etc. Applications for AR can be easily built using ThingWorx Studio [72]. ThingWorx Industrial Connectivity connects various devices providing a single source for all industrial automation data[38]. ThingWorx Analytics[39] provides analytical and predictive operations. The essential parts of ThingWorx Analytics are ThingWatcher, ThingPredictor, ThingAnalyzer, and ThingWorx Analytics Server. Finally, ThingWorx Utilities[40] allow management of devices in IoT. Their essential parts are a support for device management, process workflow, and integration on the level of IoT.

CCM Classification: External/Internal, Proprietary, De-perimeterised, Insourced/Outsourced

According to the CCM by Jericho Forum (see Section 1.1.4), ThingWorx can be categorized as both external and internal (it is deployed in PCT infrastructure by default or it can be deployed on AWS, or Microsoft Azure clouds). It is proprietary (a closed-source solution). It can also be seen as de-perimeterised (the authentication and access control are implemented by application developer, connections done in ThingWorx Foundation may

[37] https://www.microsoft.com/microsoft-hololens/en-us

[38] see https://www.kepware.com/en-us/

[39] https://www.thingworx.com/platforms/thingworx-analytics/

[40] https://www.thingworx.com/platforms/thingworx-utilities/

direct data to almost any target). Finally, it can be used as an insourced cloud service (the private cloud can be operated by the organisation's employees if required), but outsourcing is possible as well.

Nevertheless, there both the option of the external or internal deployment and the option of outsourcing or insourcing, thus, several different approaches can be used. For such options PTC offers enough experience [73] and solutions for their customers including several certifications on the side of PTC/ThingWorx, "... ThingWorx Platform delivered either at their own premises, or via our SSAE 16/SOC 2 audited on-demand centers with ISO27001:2013 certified systems and operations group with commitment to the security of our (PTC) services for our (PTC) customers" [74].

Data Analytics: Predefined, or Custom

ThingWorx Platform offers ThingWorx Analytics as its essential part. Moreover, various simple and even more complex visualization toolboxes are available in ThingWorx Studio and can be part of possibly AR application build for particular IoT device.

As it has already been mentioned above, ThingWorx Analytics contains several parts that enable data observation, prediction of future device behavior, workflow management, and others.

Besides that, ThingWorx Platform enables especially interconnection of various elements and, thus, user-developed or third party Big data analytical tools and applications can be used as they can be connected to a uniform data stream provided by ThingWorx Platform. Besides others, SAP [68] can be also connected and its analytical features can be exploited this way.

Security: Encrypted Communication, Authentication and Access Control

The ThingWorx Platform is a mean that provides uniform data transfer between a source (usually device in IoT) and a target (monitoring application, storage, etc.). Thus, there are only two potentially vulnerable items on the way. The communication line and the ThingWorx Platform itself. If we omit ThingWorx Platform and take it as safe and correctly working then the communication must be secured. It has already been mentioned above [74] that PTC supports via other tools and solutions a complex way, how to secure not only transfer of data, but their secure and safe storage, processing, etc. The way of securing is mainly in the hands of developers and their skills, from the side of ThingWorx and PTC, there is a full support.

To fulfil the security requirements, the ThingWorx Platform provides an extremely granular security model for data isolation and service execution [74]. That means in particular HTTPS authentication, delegation to Lightweight Directory Access Protocol (LDAP), industrial standards such as SAML and single sign-on, including even integration with other tools, e.g., SAP. The ThingWorx Platform internally uses an access control list to allow authorization on virtually every single operation.

Opportunities

The following opportunities according to Section 2.2 can be addressed by ThingWorx Platform with comments:

O1 *Low initial investment* — pricing policy is hidden, moreover, Czech Republic is not listed among countries available for subscription policy. Nevertheless, ThingWorx Studio is offered for at least 90 days trial (even 120 days trial is possible in particular cases). Many other services are provided online by PTC, without necessity to run locally any IT resources. Nevertheless, for serious work in a production this is not an option. Thus, it is possible to expect an initial cost to run serious development.

O2 *Outsourcing and IT service management* — all services can be outsourced and delivered by some third parties. E.g., ThingWorx Platform by PTC, data stores by other providers, etc.

O3 *Mashups* — the ThingWorx Platform is mainly devoted for uniform interconnection of data providers and data consumers. Thus, creation of a mashups later, after establishing some particular applications should not be a problem.

O5 *Scalability* — the ThingWorx Platform is initially developed as a cloud service, thus there should be no problem with scalability.

O7 *Connected vehicle* — the ThingWorx Platform can be used together with well developed applications in a way to directly support a connected vehicle via IoT and edge computing. Data gathered in a car are after initial processing transferred in the uniform way via ThingWorx Platform to applications that further process and analyse the data in order to, e.g., optimize traffic, predict malfunction, etc.

O9 *Better monitoring (transparency)* — the ThingWorx Platform tries to deliver uniform access to data streams with various target applications, thus, with proper applications the monitoring can be much simpler. Such applications can be either developed in-house, or some ready-to-use solution can be used if available.

Threats

The following threats according to Section 2.2 are softened or should be addressed in ThingWorx Platform applications:

T1 *Dependency and vendor lock-in* — the ThingWorx Platform is a proprietary SW, thus, even if developing our own applications over this platform, it means in many ways a danger that if anything happens to framework, it is necessary to rebuild even a large portion of application ecosystem developed.

T3 *Data lock-in, data confidentiality, and shared reputation* — this may be a threat only if data stores provided by PTC are used. On the other hand, routing data from IoT devices to ThingWorx hosted by PTC and then back is not feasible neither. Nevertheless, data can be encrypted by functions provided within ThingWorx Platform. However, the encryption may slow down the execution of later data processing.

T4 *Non-transferable responsibility* — if the ThingWorx Platform is operated locally then there is no problem with non-transferable responsibility. Nevertheless, if some other cloud provider is used (e.g., PTC, Amazon) then there is a problem, that must be solved by suitable agreements.

T5 *Data transfer bottlenecks* — the ThingWorx Platform enables large scale networks and even quite large data amounts to be transferred from quite distant places. If the application is sensitive on proper timing of data delivery then it may be a problem. Nevertheless, this is a general problem of cloud computing.

T6 *Performance unpredictability in multi-tenant environments* — the ThingWorx Platform is not devoted for real-time operation in a sense of committing any time intervals, thus this should not be a problem.

Summary

ThingWorx Platform offers many possibilities, how devices of IoT can be monitored, controlled, presented to users, analysed, and maintained. This comprises not only one particular device, but a series of devices and a whole workflow coupled with such tasks. Even if ThingWorx Platform offers many predefined and prepared utilities and tools, it especially provides a unified and uniform way to access data provided by IoT and to build various applications. Such applications can start from monitoring and failure prediction to AR applications targeting either servicing staff or end-users of a customer. We can say, it is a large framework enabling edge computing and handling of devices in IoT in a uniform way providing many (development) tools, utilities, and application components to create required applications.

It is a well established platform. Thus, it enables reuse of existing elements, e.g. computer-aided design (CAD) files to build AR applications, or storage and analytical tools well connected with SAP. Moreover, it offers ready-to-use building blocks to develop customer applications of various purposes and targeting.

3.2.2 Siemens MindSphere

In July 2016, Siemens launched a platform for industrial cloud called "MindSphere – the cloud-based, open IoT operating system from Siemens". According to [75], MindSphere is an open cloud platform offered in the form of PaaS which is designed as an IoT operating system with data analytics and connectivity capabilities, tools for developers, applications and services. It should help to evaluate and utilise industrial data and to gain breakthrough insights, e.g., to drive the performance and optimization of assets for maximized uptime. Despite of the fact that "MindSphere offers customers a development environment in which they can integrate their own applications and services" [75], MindSphere and its MindApps, which are Siemens applications running on MindSphere, are currently (June 2017) still in a closed beta version with limited access without any application store and application development documentation[41].

In this section, Siemens MindSphere will be analysed and evaluated for the comparison in the current closed beta version, together with SAP Cloud Platform based on SAP HANA for data analytics. Both of these cloud computing solutions are utilising Cloud Foundry platform[42], so they can be deployed in cloud environments supporting Cloud Foundry[43]. While Siemens MindSphere is not yet publicly available for Cloud Foundry, SAP Cloud Platform is strongly utilising Cloud Foundry. Moreover, SaaS products by SAP, such as SAP S/4 HANA or SAP Business ByDesign, are well-integrated with Cloud Foundry and ready-to-use in its environment.

Characteristic Service Model: SaaS (PaaS prospectively)

Currently, MindSphere is implementing SaaS cloud service model where customers are provided with a SW running in cloud (MindSphere Launchpad). Despite of the fact that a customer needs to install customisable edge devices (MindConnect elements) that would be ready to perform various tasks, these devices just report data to the cloud and do not host any cloud service by themselves. Moreover, the development of custom applications running in the MindSphere cloud (MindApps) is not yet supported in the closed beta

[41] see https://community.plm.automation.siemens.com/t5/x/x/m-p/409469 and https://community.plm.automation.siemens.com/t5/x/x/m-p/412773

[42] https://www.cloudfoundry.org/

[43] Actually, Siemens MindSphere is based on SAP HANA Cloud Platform which is utilising Cloud Foundry.

version, so only predefined applications implemented by Siemens are currently available as SaaS.

However, according to [75], MindSphere is designed for PaaS service model and both the customisation of edge devices and the development of custom cloud applications running on MindSphere platform will be available in the near future.

Cloud Architecture: Edge

According to [76], MindSphere architecture is structured into three layers: MindSphere cloud, MindConnect elements, and industrial assets. In the middle layer of MindConnect elements, MindConnect Nano and smaller MindConnect IoT2040 devices read monitoring data of industrial assets from SIMATIC S7-300/400 PLCs and OPC-UA servers at the bottom layer via an industrial Ethernet network. After the MindConnect elements establish a connection to MindSphere cloud via Internet (another Ethernet interface), the collected data from assets are transferred into MindSphere cloud. At the top layer, MindSphere cloud offers means to monitor asset status from the collected and transferred data via MindSphere Launchpad web user interface.

MindSphere Launchpad is an entry point to the user interfaces (i.e., MindApps) for data visualization and configuration. MindApps can be opened from an up-to-date browser with HTML5 capabilities. In MindSphere, users can create, configure, onboard, and visualize a "digital twin" of an asset via graphical interfaces. [76]

Currently, in its closed beta version, MindSphere Launchpad provides three system MindApps applications: MindSphere Asset Configuration, MindApp Fleet Manager, and MindSphere User and Customer Management. According to [76], the Asset Configuration offers means to perform configuration on an asset and MindConnect Nano/IoT2040 device to define the asset's monitoring data structure and properties, to setup connections of the MindConnect Nano/IoT2040 device to monitored assets and MindSphere cloud, and to manage metadata on the assets (e.g., their geographical location). Fleet Manager is used for getting an overview of existing assets and their basic information as well as visualization of asset data including detailed data analysis – to look at various variables with various aspects and view them in three different types of charts (line, pie, and bar charts) in different time frames. User of the Fleet Manager can also create manual requests, such as warnings or maintenance requests, or define rules for automatic generation of the requests. Finally, there are MindApps for User Management application to create and manage MindSphere Launchpad users of two roles ("admin" and "user") and Customer Management application where "admin" users can create accounts for their customers and assign them their assets.

This architecture is in accordance with the edge cloud computing where data are extracted from assets by edge devices (running MindConnect elements) and transported into cloud for further processing (MindSphere cloud). IoT edge devices are managed by MindSphere Asset Configuration. It is neither a static architecture (the edge device are participating dynamically) nor a fog computing architecture (edge devices just serve to other services in the global cloud).

CCM Classification: External/Internal, Proprietary, De-perimeterised, Insourced

According to the CCM by Jericho Forum (see Section 1.1.4), MindSphere in the closed beta version can be categories as both external and internal (it is deployed in Siemens IT infrastructure by default or can be deployed on a private cloud), proprietary (a closed-source solution provided by Siemens including HW devices for MindConnect elements), de-perimeterised (the authentication and access control are implemented by vendor in

MindSphere User and Customer Management applications, i.e., outside of an organisation's IT infrastructure perimeter), and insourced cloud service (the private cloud can be operated by the organisation's employees if required).

Still, this categorisation is very informal and unsettled as MindSphere is in the closed beta version where it is available to selected partners only and probably highly customised to their needs. In these cases, the individually customised deployments may include various custom MindApps deployed in hybrid clouds, both internal and external, insourced and outsourced, and integrating open technologies, such as from Cloud Foundry, with proprietary MindSphere.

Data Analytics: Predefined, or Big Data (with SAP HANA Cloud Platform)

Internally, MindSphere is based on SAP HANA Cloud Platform[44], that is SAP Cloud Platform with SAP HANA in-memory database available as PaaS. SAP HANA provides a cloud runtime environment for applications storing, manipulating, and querying data according to the concepts of Big data and Fast data discussed in Section 1.2.3. Despite of this fact, the closed beta version of MindSphere in its MindApp Fleet Manager application enables its users only with elementary data views, visualisations, and analytics. According to [76], it is possible to filter data by their source, time, and aspects, to view their various variables with the aspects, numerically or in three different types of charts (line, pie, and bar charts) in different time frames. User of the Fleet Manager can also create manual requests or define rules automatically generating the requests, such as warnings or maintenance requests.

The analytic features described above are quite simple with predefined ways how to query, view, and analyse the data. This analytics works quite well, especially for time series, that is for sequences of measurements produced by data sources over time [76]. However, the analytics in MindApp Fleet Manager application will be hardly sufficient for a large-scale monitoring, e.g., in a manufacturing cloud. Contrary to that, the ability to use SAP HANA Cloud Platform for the data analytics and visualisation would bring full support of Big data analytics and a very good integration with Big data processing systems, such as with SAP Vora[45]. We expect such Big data analytics will be available in MindSphere in near future versions (or in the case of highly customised deployments of the closed beta version).

Security: Encrypted Communication and Storage, Authentication, Access Control

Communication between MindConnect elements, i.e., MindConnect Nano/IoT2040 devices, and MindSphere cloud is encrypted via HTTPS. On each device, there is only one HTTPS outbound network port opened (i.e., no inbound or other outbound connections) and a configuration is done via a local HW port or remotely from MindSphere Asset Configuration in MindSphere Launchpad. The authentication and access control are managed by MindSphere User and Customer Management in MindSphere Launchpad with two predefined user roles ("admin" and "user"). Unfortunately, no information is available on an advanced configuration of these security features, such as on setting a custom HTTPS certificate for the encrypted communication, custom user roles and other access control settings, or utilising of external identity management and authentication services for single sign-on, etc.

[44] `https://www.sap.com/products/hana-enterprise-cloud.html`

[45] `https://www.sap.com/products/hana-vora-hadoop.html`

Also cloud infrastructure security is not discussed in details in the closed beta version of MindSphere, although, available security features can be guessed from underlying technologies, i.e., SAP HANA Cloud Platform and Cloud Foundry. For example, SAP Cloud Platform [77] implements many security measures, such as application and network sandboxing, customer and network segregation, secure communication, secure application containers, system hardening, client media encryption, and backup and log security. Similarly, Cloud Foundry [78] can offer virtualisation container isolation and encryption as well as identity management and authentication services.

Opportunities

The following opportunities according to Section 2.2 can be addressed by Siemens MindSphere and SAP Cloud Platform with comments:

O1 *Low initial investment* — Siemens MindSphere can be deployed in a minimal configuration of one MindAccess User license[46] for a public MindSphere cloud deployment and one MindConnect Nano/IoT2040 device where industrial assets such as PLCs can be connected. The MindAccess User license enables a customer to access and use MindSphere Platform and the included MindApps for a fixed monthly fee (for the first 50 users of the customer) and a monthly usage fee depending on the configuration (additional users, data model and number of connected assets, usage of MindApps). In April 2017, the cost of one MindConnect Nano device was 990 EUR and the cost of the MindAccess User license was 150 EUR per month[47]. In the case of a private cloud deployment of MindSphere, e.g., for security reasons, the initial investment would be much higher.

O2 *Outsourcing and IT service management* — By default, Siemens MindSphere is a ready-to-use solution provided in a public cloud deployment, so it is outsourced by Siemens. Although MindSphere is based on Cloud Foundry with SAP HANA Cloud Platform which should be deployable on any Cloud Foundry compatible IT infrastructure or IaaS cloud service, moving from Siemens to another vendor may not be easy for many reasons, especially in the current closed beta version of MindSphere (proprietary protocols, insufficient documentation, etc.).

O3 *Mashups* — Currently, the closed beta version of MindSphere is not ready for integration with another cloud services provided by Siemens or another vendors. Therefore, mashups are problematic.

O5 *Scalability* — As MindSphere is running on Cloud Foundry with SAP HANA Cloud Platform, its scalability is very good.

O9 *Better monitoring (transparency)* — Siemens MindSphere is designed and built for gathering, processing, storing, and analytic presentation and visualisation of monitoring data of connected industrial assets. Therefore, it can significantly improve monitoring of the assets in manufacturing and increase transparency of running production processes.

Currently, Siemens MindSphere is just an industrial data monitoring and analysis platform without full support of CMfg as defined in Section 2.1.2). Therefore, Siemens MindSphere cannot address opportunities O7 (Connected vehicle) and O8 (Agile manufacturing)

[46] see `https://support.industry.siemens.com/cs/products/9ac2513-3mj11-4nd4`

[47] see `https://community.plm.automation.siemens.com/t5/x/x/ta-p/403910`

that may be interesting for manufacturing industry. However, with going public and enabling MindApps application development for MindSphere, there will probably emerge also better support for CMfg and integration with other Siemens products, e.g., for automotive manufacturing.

Threats

The following threats according to Section 2.2 are softened or should be addressed in Siemens MindSphere and SAP Cloud Platform applications:

T1 *Dependency and vendor lock-in* — With Siemens MindSphere, there is a strong dependency on Siemens technologies (e.g., MindConnect Nano/IoT2040 are proprietary closed HW devices) as well as on underlying commercial products in SAP HANA Cloud Platform. The vendor lock-in is possible.

T3 *Data lock-in, data confidentiality, and shared reputation* — In the case of a public cloud deployment of Siemens MindSphere, it may be difficult to protect data in accordance with well-established security policies of a customer's organisation as well as to migrate data to another cloud computing vendor with a different product. However, the issue can be solved by using a private cloud based on Cloud Foundry and SAP HANA Cloud Platform for MindSphere where the data are fully controlled by the customer's organisation.

T4 *Non-transferable responsibility* — In the case of a private cloud deployment of Siemens MindSphere, non-transferable responsibilities are not problem. However, the situation may be different in the case of the default public cloud deployment where the responsibilities must be formally defined in contracted Service Level Agreements (SLAs).

T5 *Data transfer bottlenecks* — For communication between MindConnect elements, i.e., MindConnect Nano/IoT2040 devices, and public MindSphere cloud, a direct or forwarded Internet connection is required. This connection can be a data transfer bottleneck due to its limited capacity or availability. However, a temporarily missing or insufficient Internet connection should not be problem, as the MindConnect elements are able to buffer data if off-line and send them as soon as a sufficient Intenret connection is available.

T6 *Performance unpredictability in multi-tenant environments* — As MindSphere cloud is utilised only for monitoring data analyses (filtering, presentation, and visualisation), not for real-time or near-real-time task such as virtual programmable logic controller (VPLC) or VRC, the performance unpredictability is not a valid threat in this case.

Summary

Although Siemens MindSphere is built on SAP HANA Cloud Platform and Cloud Foundry that are utilised as PaaS/IaaS, it is a closed proprietary cloud service. The MindSphere platform declares itself to be PaaS for MindApps development but it is actually, in the current closed beta version, more a SaaS solution without publicly available development documentation and tools. These two disadvantages are considered a big handicap and should be eliminated. Moreover, MindSphere is not suitable for full-featured manufacturing cloud, as it is primarily designed for monitoring rather than controlling of connected industrial assets. Finally, MindSphere currently allows only elementary monitoring data analyses in predefined MindApps and development of custom MindApps with Big data analytics is problematic due to missing documentation, tools, and no well-established integration with Big data processing SW.

Despite disadvantages above, Siemens MindSphere is an interesting project with meaningful applications for production asset monitoring and management in manufacturing industry, especially where another Siemens technologies are utilised for the assets, e.g., as PLCs.

3.2.3 GE Predix

Predix by GE is a cloud computing platform for the collection, analysis, and presentation of data from industrial machines to predict potential problems, conduct preventative maintenance, and reduce unplanned downtimes [79].

Characteristic Service Model: PaaS

As described in [79], Predix Cloud is a core of the Predix platform for industrial Internet (a network of industrial devices) which consists of a scalable cloud infrastructure serving as a basis for PaaS. Developers utilise the Predix Cloud platform to create, deploy, and run industrial Internet applications, both predefined by Predix and custom implemented in Java, Matlab, or Python programming languages. Predix itself does not provide a cloud core platform or an infrastructure as services, i.e., PaaS/IaaS; that is delegated to underlying Cloud Foundry framework[48], so Predix platform can run on any public, private, or hybrid cloud infrastructure which supports the Cloud Foundry technologies. Also SaaS is not the service model directly offered by Predix as the services are usually custom implemented or composed from the Predix platform components, despite the fact that there exist several predefined cloud applications.

Cloud Architecture: Edge

In Predix, the cloud architecture consists of components of five types: Predix Machine, Predix Connectivity, Predix EdgeManager, Predix Cloud, and Predix Services.

Predix Machine is a SW, which communicates with the industrial assets and with Predix Cloud and where local applications are running, such as edge analytics. Predix Connectivity can be utilised to provide Predix Machine components with network connectivity to Predix Cloud if a direct Internet connection is not readily available (otherwise, Predix Machine and Predix Cloud are connected directly via Internet, without Predix Connectivity). Predix EdgeManager manages edge devices that are running Predix Machine components. Predix Cloud is a global cloud infrastructure for running Predix Services and a marketplace of catalogue services where developers can publish their own services as well as consume and integrate services from third parties. And finally, Predix Services are industrial services that developers can use to build, test, and run industrial internet applications.

This architecture is in accordance with the edge cloud computing where data are extracted from edge devices (running Predix Machine) and transported into cloud for further processing (transported via Internet or by Predix Connectivity to Predix Cloud to be processed by Predix Services). IoT edge devices are managed by Predix EdgeManager. It is neither a static architecture (the edge devices are participating dynamically) nor a fog computing architecture (edge devices just serve other services in the global cloud).

[48] https://www.cloudfoundry.org/

CCM Classification: Internal, Proprietary, De-perimeterised, Insourced

According to the CCM by Jericho Forum (see Section 1.1.4), Predix can be categories as internal (it can be deployed on a private cloud running Cloud Foundry), proprietary (a closed-source solution provided by GE), de-perimeterised (the authentication and access control are implemented by predefined User Account and Authentication Service and Access Control Service, respectively, both running in Predix Cloud managed a cloud provider, that is outside of a customer's IT infrastructure perimeter), and insourced cloud service (the private cloud can be operated by the customer's employees if required).

In the case of non-private cloud deployments of Predix Cloud on Cloud Foundry PaaS/IaaS service provided in public or hybrid cloud, the classification may be different, e.g., the Predix cloud service may be external and outsourced (data can be stored and operated by a third party of the IaaS cloud provider).

Data Analytics: Custom

In Predix, the entry point for all data incoming from various data sources is an ingestion pipeline. According to [79], the ingestion pipeline enables data to be received via HTTP streaming for real- or near-real-time data (Fast data, see Section 1.2.3) or File Transfer Protocol (FTP) for more batch-style processing. Moreover, before the data is stored, it can be processed in the pipeline, e.g., annotated, combined with other data, processed as complex events (the system is looking for a combination of certain types of events to create a higher-level business event), etc. The data can be stored in a distributed scalable data store for time series (suitable for sensor data with series of measurement values), a binary large object (BLOB) store (for large image data up to 10 GB), and in PostgreSQL[49] open-source relational database (for relational data).

Analyses on the data can be performed in orchestrations of multiple predefined and custom analytics services defined in an analytic catalogue. The analytics services can perform operational analysis of the current data and historical analysis of data from the data stores above. There is a set of predefined analytics services in the catalogue that include complex algorithm implementations in areas such as anomaly detection and ML [79]. Moreover, another custom analytics services can be written in Java, Matlab, and Python. The orchestrations of analytics services are described in Business Process Modelling Notation (BPMN), version 2.0, and executed by an orchestration runtime service on demand. By the orchestration of the services for both operational analysis and historical analysis, it is possible to implement complex trend analyses and others.

As described above, the Predix ingestion pipeline focus on Fast data ingestion, transportation, and processing. The time series and BLOB data stores support storage of data from the ingestion pipeline as Big data. However, Predix is not a Big data analytics cloud platform as described in Section 1.2.3 and thorough Big data/Fast data analytics should be performed by specialised Big data processing tools, such as Apache Spark[50], that would be called from the custom analytics service.

Security: Encrypted Communication, Identities, Authentication, Access Control

According to [79], data encryption and authentication/authorisation for access control is performed by Predix Machine component. In order to provide end-to-end security, Predix

[49] https://www.postgresql.org/

[50] https://spark.apache.org/

Machine supports a certificate management to provide Secure Sockets Layer (SSL) connections to the Predix Cloud. Moreover, there is a support for security profiles, authentication, identity management, and access control by two application security services: User account and authentication (UAA) Service and Access Control Service.

By means of UAA Service, Predix applications are able to identify and authenticate their users directly, or by System for Cross-domain Identity Management (SCIM) and OAuth standards to handle identity management and authentication, respectively. Additionally, UAA supports SAML, which enables users to login using third-party identity providers. Predix Access Control service is a policy-driven authorization service that enables applications to create access restrictions to resources based on a number of criteria, well integrated with UAA. The policy language is based on JavaScript Object Notation (JSON) and was developed as an answer to the deficiencies in eXtensible Access Control Markup Language (XACML). [79]

The Predix security implementation described above focuses on secure data transport from Predix Machine to cloud and secure access to the cloud services by their users. It does not deal with cloud infrastructure security, for example, with a secure and reliable data storage, which may be covered by underlying Cloud Foundry technology. Cloud Foundry [78] can offer a virtualisation container isolation and encryption as well as its own UAA service that can be shared with Predix. However, in the case of full outsourcing of both Cloud Foundry PaaS/IaaS and Predix PaaS, the security features may not be enough to keep data secure according to well-established security policies of most of industrial organisations.

Opportunities

The following opportunities according to Section 2.2 can be addressed by Predix with comments:

O1 *Low initial investment* — Both Predix and underlying Cloud Foundry can be installed with minimal costs. However, there may be additional investments to new dedicated HW for Predix Machine components if an existing compatible HW is not available.

O2 *Outsourcing and IT service management* — Predix is easy to deploy and based on an open technology by Cloud Foundry which makes it easy to outsource if necessary. It should be noted that in the case of outsourcing, there can be a different classification according to the CCM by Jericho Forum and another security issues (see above).

O3 *Mashups* — It is quite easy to mix and integrate various cloud services in Predix on demand, for example, for data analytics as described above.

O5 *Scalability* — Both Predix services in PaaS and underlying Cloud Foundry in PaaS or IaaS service models are scalable.

O9 *Better monitoring (transparency)* — Predix strongly supports monitoring of industrial assets, their data are monitored by Predix Machine components and sent to Predix cloud for analyses.

As Predix is focused on monitoring and analytics, not on the full feature-set of CMfg (see Section 2.1.2), it probably cannot address opportunities O7 (Connected vehicle) and O8 (Agile manufacturing) that may be interesting for manufacturing industry.

Threats

The following threats according to Section 2.2 are softened or should be addressed in Predix applications:

T1 *Dependency and vendor lock-in* — By utilisation of open Cloud Foundry technology for PaaS/IaaS, there is no vendor lock-in at this level. Yet, at PaaS level, Predix is a closed proprietary solution where the vendor lock-in should be recognised as a valid threat.

T3 *Data lock-in, data confidentiality, and shared reputation* — This threat is minimised by underlying open Cloud Foundry technology for PaaS/IaaS. The Predix can be deployed as a private cloud implemented in-house and operated inside a customer's organisation.

T4 *Non-transferable responsibility* — Similarly as the threat above, also the non-transferable responsibility is not problem in Predix.

T5 *Data transfer bottlenecks* — Connections of Predix Machines into Predix cloud may cause possible data transfer bottlenecks. However, this issue can be solved by Predix Connectivity.

T6 *Performance unpredictability in multi-tenant environments* — As Predix cloud is utilised only for monitoring and data analyses, not for real-time or near-real-time tasks such as VPLC or VRC, the performance unpredictability is not a valid threat in this case.

Summary

Due to good and flexible architecture with many predefined and customisable components and for utilisation of open Cloud Foundry technology for PaaS/IaaS, Predix is a very good cloud solution for monitoring of industrial assets and analyses of the monitoring data especially in combination with other data, such as from strategy or business management. Predix is not suitable for full-featured CMfg, as its Predix Machine is primarily designed for monitoring rather than controlling of connected industrial assets.

3.2.4 Conclusion

Although none of the compared cloud solutions fully supports CMfg as defined in Section 2.1.2), they can be successfully utilised in manufacturing industry for monitoring of critical assets in the production, observing the progress of production processes, manufacturing machines wear and tear, for analysing incidents and optimizing the production. In the fast processing of large amount of data generated by assets, cloud-based Big data processing and analytics bring significant cost advantages and ability to make operational and strategic decisions on the actual data. This Big data processing and analytical features are (or will be) supported by all of the compared cloud solutions. All the cloud solutions posses also the ability to run in both public and private cloud deployments, which is important for minimising threats discussed in Section 2.2. So in these aspects, all three cloud solutions are quite mature.

Yet, from the cloud solutions for manufacturing industry selected in Section 3.2, we would recommend to choose GE Predix as it is a well-established solution (contrary to both PTC Thingworx and Siemens MindSphere) with excellent documentation and based on the open Cloud Foundry platform without another proprietary dependencies (contrary to Siemens MindSphere which is based on SAP HANA Cloud Platform with minimal documentation), and also with flexible data analytics which can seamlessly integrate Big data processing SW and another cloud services (contrary to both PTC Thingworx and Siemens MindSphere).

From other cloud solutions in Section 3.1 and according to the overall results of the comparison shown in Table 3.1, IBM BlueMix / Watson IoT Platform is the most promising solution for possible development of CMfg.

4 Executive Summary

Cloud computing aims to solve well-known problems of information technology (IT) systems, such as high maintenance and IT infrastructure costs, low scalability and agility, problematic outsourcing, and others. To address these issues, cloud computing employs progressive techniques, such as distributed computing, virtualisation, virtual-private networking, etc. A combination of these techniques enables to build cloud computing systems with six essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, measured services, and multi-tenancy. According to IT components (infrastructure, platform, and software (SW)) that are implemented by a cloud computing system, the system implements one of the three service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Moreover, according to deployment of hardware (HW) and SW running the cloud system, we can distinguish private, public, or hybrid cloud, owned by a customer, a provider, or both of them. In practice, security in cloud computing is significantly affected by different combinations of those service models and deployments, together with a physical location of the cloud, its openness, responsibility for authentication and access control to resources in the cloud, and a delivery of the cloud services.

Emerging trends in the cloud computing are trying to address even higher demands on agility, flexibility, and scalability. In edge computing, a cloud infrastructure utilises computing devices that are at the cloud edge from the point of view of a cloud provider, so close to customers. The edge devices are usually managed (or also owned) by a customer at his/her locations and they can, for example, preprocess input data before sending them into the cloud, manage sensitive data that cannot be stored in the cloud, or directly provide some cloud services with high reliability even with erroneous and unstable network connection to the cloud. In the case of fog computing, those edge devices provide their services to other devices and users (edge or non-edge) in the cloud which becomes “a fog” of cloud services. The edge and fog computing frequently utilise Internet of Things (IoT) devices, e.g., to monitor and control industrial assets in manufacturing, which results into new service models, such as Robot as a Service (RaaS). Moreover, the employment of edge devices that gather or produce a lot of data requires also better data processing and analytics in the cloud. Big data approaches deal with high volume data, while Fast data approaches aim at velocity of data streams for real-time or near real-time processing and analytics of the data. In these cases, cloud computing implements Data as a Service (DaaS) or “Big Data ... as a Service” service models.

There are two levels of the utilisation of cloud computing in manufacturing industry: (1) smart manufacturing with cloud computing and (2) cloud manufacturing (CMfg). In the first approach, the cloud computing just helps with well-established tasks in a manufacturing company. For example, smart manufacturing with cloud computing can improve Business Process Management (BPM) and other business applications or provide data migration and load balancing, virtualisation, monitoring and Big data analytics, implement a virtual factory (VF), or prognostics and health management (PHM). Contrary to the smart manufacturing with cloud computing, the CMfg utilises edge and fog computing to spread cloud infrastructure towards industrial assets. For example, in the case of data analytics, edge computing would employ IoT devices connected to the industrial assets not only for reading their data and sending them into the cloud, but also for evaluation of the data and quick response operations performed by the devices. In the case of fog computing, there would be no visible border between the centre and the edge of a cloud with seamlessly integrated cloud services provided by both the central cloud infrastructure and the edge devices. Currently, the fully featured CMfg is a subject of many research projects.

To analyse suitability of cloud computing for automotive/electronics manufacturing industry, we categorised the existing cloud computing solutions and evaluated how they address several identified opportunities and threats. Detailed results of the comparison were available in Chapter 3 and outlined in Table 3.1. The following publicly available cloud services for manufacturing industry were analysed and compared: AWS IoT (Sec 3.1.1); IBM BlueMix, Watson IoT (Sec 3.1.2); Microsoft Azure IoT (Sec 3.1.3); Google Cloud IoT (Sec 3.1.4); SAP Cloud Platform for IoT (Sec 3.1.5); Mnubo (Sec 3.1.6); PTC ThingWorx (Sec 3.2.1); Siemens MindSphere (Sec 3.2.2); and GE Predix (Sec 3.2.3).

Based on a consultation with target audience of this report, the last three cloud computing services have been analysed in more details. From these three selected cloud computing services, we would recommend to choose General Electric (GE) Predix as it is a well-established solution (contrary to both PTC Thingworx and Siemens MindSphere) with excellent documentation and based on the open Cloud Foundry platform without another proprietary dependencies (contrary to Siemens MindSphere which is based on SAP HANA Cloud Platform). Moreover, there is also flexible data analytics which can seamlessly integrate Big data processing SW and cloud services (contrary to both PTC Thingworx and Siemens MindSphere). From other cloud solutions, IBM BlueMix / Watson IoT Platform is the most promising solution for possible development of CMfg.

5 Conclusion and Recommendation

In this report, the state of the art of cloud computing in manufacturing industry has been discussed. After a short introduction into cloud computing terminology and concepts in Chapter 1, current trends in cloud computing applications in manufacturing industry have been discussed in Chapter 2. Existing solutions of cloud computing for manufacturing have been analysed and compared in Chapter 3.

Cloud computing brings new opportunities to manufacturing industry as described in Section 2.1. New cloud computing systems can be created and well-established information technology (IT) systems can be migrated onto the cloud computing technology to address these opportunities. Before taking a final decision to utilise the cloud computing technology, especially the decision to migrate a production system into the cloud, however, several things need to be considered. A manufacturing organisation should have to consider, among other factors, the practical applicability of cloud computing, possible threats, and security aspects described in this report. Many of these factors were discussed in Chapter 2. From the IT security point of view, we would recommend to perform security risk assessment according to Cloud Security Alliance (CSA) (see Section 2.3.2), to adopt relevant security control and compliance models or require their verifiable adoption by cloud providers, to implement information management and data security, and to use open cloud solutions and technologies that are easier to deploy privately and control in terms of security. Moreover, common IT security policies must be implemented and enforced, e.g., to protect local IT infrastructure and devices accessing the cloud.

In the comparison of the existing cloud computing solutions for manufacturing, based on a consultation with target audience of this report, the three cloud computing solutions have been analysed in more details. From these three selected cloud computing solutions, we would recommend to choose General Electric (GE) Predix as it is a well-established solution with excellent documentation and based on the open Cloud Foundry platform without another proprietary dependencies, and also with flexible data analytics which can seamlessly integrate Big data processing software (SW) and cloud services. From other cloud solutions, IBM BlueMix / Watson IoT Platform has been considered the most promising solution for possible development of cloud manufacturing (CMfg).

Although the cloud computing solutions above are good, the most optimal cloud solution would be, at least from the point of view of flexibility and security, the following: internal, privately deployed, open, perimeterised, and insourced (see Section 1.1.4). However, such an optimal cloud solution is not currently provided anywhere and it is necessary to make a compromise between costs and security: to use a deperimeterised cloud of a trustworthy provider where all security features are implemented correctly; to use hybrid deployment with sensitive data managed by “edge” devices in an organisation’s perimeter where the appropriate security policies can be better enforced; and to outsource cloud IT service management to a service provider or a trustworthy third party to consume services without additional costs.

Bibliography

[1] B. Furht and A. Escalante, *Handbook of Cloud Computing*, 1st ed. Springer Publishing Company, Incorporated, 2010. ISBN 1441965238, 9781441965233. [Online]. Available: http://dx.doi.org/10.1007/978-1-4419-6524-0

[2] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared," in *2008 Grid Computing Environments Workshop*, Nov. 2008. doi: 10.1109/GCE.2008.4738445. ISSN 2152-1085 pp. 1–10. [Online]. Available: http://dx.doi.org/10.1109/GCE.2008.4738445

[3] P. M. Mell and T. Grance, "The NIST definition of cloud computing," National Institute of Standards & Technology, Gaithersburg, MD, United States, Tech. Rep. SP 800-145, 2011. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[4] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Information Sciences*, vol. 305, pp. 357–383, 2015. doi: 10.1016/j.ins.2015.01.025. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025515000638

[5] "Security guidance for critical areas of focus in cloud computing v3.0," Cloud Security Alliance, Tech. Rep., 2011. [Online]. Available: http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[6] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," *IEEE Internet Computing*, vol. 14, no. 5, pp. 14–22, Sep. 2010. doi: 10.1109/MIC.2010.86. [Online]. Available: http://dx.doi.org/10.1109/MIC.2010.86

[7] "Jericho Forum Cloud Cube Model, version 1.0: Select cloud type for secure collaboration," The Open Group Jericho Forum, Tech. Rep. W126, 2009. [Online]. Available: https://www2.opengroup.org/ogsys/catalog/W126

[8] V. Chang, D. Bacigalupo, G. Wills, and D. De Roure, "A categorisation of cloud computing business models," in *Proceedings of the 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing*, ser. CCGRID '10. Washington, DC, USA: IEEE Computer Society, 2010. doi: 10.1109/CCGRID.2010.132. ISBN 978-0-7695-4039-9 pp. 509–512. [Online]. Available: http://dx.doi.org/10.1109/CCGRID.2010.132

[9] I. Foster, "What is the grid? – a three point checklist," *GRIDtoday*, vol. 1, no. 6, Jul. 2002. [Online]. Available: http://www-fp.mcs.anl.gov/~foster/Articles/WhatIsTheGrid.pdf

[10] M. Milenkovic, S. H. Robinson, R. C. Knauerhase, D. Barkai, S. Garg, V. Tewari, T. A. Anderson, and M. Bowman, "Toward internet distributed computing," *Computer*, vol. 36, no. 5, pp. 38–46, May 2003. doi: 10.1109/MC.2003.1198235. [Online]. Available: http://dx.doi.org/10.1109/MC.2003.1198235

[11] J. W. Ross and G. Westerman, “Preparing for utility computing: The role of IT architecture and relationship management,” *IBM Systems Journal*, vol. 43, no. 1, pp. 5–19, 2004. doi: 10.1147/sj.431.0005. [Online]. Available: http://dx.doi.org/10.1147/sj.431.0005

[12] J. O. Kephart and D. M. Chess, “The vision of autonomic computing,” *Computer*, vol. 36, no. 1, pp. 41–50, Jan. 2003. doi: 10.1109/MC.2003.1160055. [Online]. Available: http://dx.doi.org/10.1109/MC.2003.1160055

[13] A. Davis, J. Parikh, and W. E. Weihl, “EdgeComputing: Extending enterprise applications to the edge of the internet,” in *Proceedings of the 13th International World Wide Web Conference on Alternate Track Papers & Posters*, ser. WWW Alt. ’04. New York, NY, USA: ACM, 2004. doi: 10.1145/1013367.1013397. ISBN 1-58113-912-8 pp. 180–187. [Online]. Available: http://doi.acm.org/10.1145/1013367.1013397

[14] T. H. Luan, L. Gao, Z. Li, Y. Xiang, and L. Sun, “Fog computing: Focusing on mobile users at the edge,” *CoRR*, vol. abs/1502.01815, 2015. [Online]. Available: http://arxiv.org/abs/1502.01815

[15] P. Garcia Lopez, A. Montresor, D. Epema, A. Datta, T. Higashino, A. Iamnitchi, M. Barcellos, P. Felber, and E. Riviere, “Edge-centric computing: Vision and challenges,” *SIGCOMM Comput. Commun. Rev.*, vol. 45, no. 5, pp. 37–42, Sep. 2015. doi: 10.1145/2831347.2831354. [Online]. Available: http://doi.acm.org/10.1145/2831347.2831354

[16] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, “An overview of fog computing and its security issues,” *Concurrency and Computation: Practice and Experience*, vol. 28, no. 10, pp. 2991–3005, 2016. doi: 10.1002/cpe.3485. [Online]. Available: http://dx.doi.org/10.1002/cpe.3485

[17] L. M. Vaquero and L. Rodero-Merino, “Finding your way in the fog: Towards a comprehensive definition of fog computing,” *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 5, pp. 27–32, Oct. 2014. doi: 10.1145/2677046.2677052. [Online]. Available: http://doi.acm.org/10.1145/2677046.2677052

[18] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, “Fog computing and its role in the internet of things,” in *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, ser. MCC ’12. New York, NY, USA: ACM, 2012. doi: 10.1145/2342509.2342513. ISBN 978-1-4503-1519-7 pp. 13–16. [Online]. Available: http://doi.acm.org/10.1145/2342509.2342513

[19] M. Lom, O. Pribyl, and M. Svitek, “Industry 4.0 as a part of smart cities,” in *2016 Smart Cities Symposium Prague (SCSP)*, May 2016. doi: 10.1109/SCSP.2016.7501015 pp. 1–6. [Online]. Available: http://dx.doi.org/10.1109/SCSP.2016.7501015

[20] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010. doi: 10.1016/j.comnet.2010.05.010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128610001568

[21] K. Kirkpatrick, “Software-defined networking,” *Commun. ACM*, vol. 56, no. 9, pp. 16–19, Sep. 2013. doi: 10.1145/2500468.2500473. [Online]. Available: http://doi.acm.org/10.1145/2500468.2500473

[22] J. Schlick, “Cyber-physical systems in factory automation – towards the 4th industrial revolution,” in *2012 9th IEEE International Workshop on Factory Communication Systems*, May 2012. doi: 10.1109/WFCS.2012.6242540. ISSN Pending pp. 55–55. [Online]. Available: http://dx.doi.org/10.1109/WFCS.2012.6242540

[23] A. Vick, C. Horn, M. Rudorfer, and J. Krüger, “Control of robots and machine tools with an extended factory cloud,” in *2015 IEEE World Conference on Factory Communication Systems (WFCS)*, May 2015. doi: 10.1109/WFCS.2015.7160575 pp. 1–4. [Online]. Available: http://dx.doi.org/10.1109/WFCS.2015.7160575

[24] Y. Chen, Z. Du, and M. García-Acosta, “Robot as a Service in cloud computing,” in *2010 Fifth IEEE International Symposium on Service Oriented System Engineering*, Jun. 2010. doi: 10.1109/SOSE.2010.44 pp. 151–158. [Online]. Available: http://dx.doi.org/10.1109/SOSE.2010.44

[25] Q. H. Vu, T. V. Pham, H. L. Truong, S. Dustdar, and R. Asal, “DEMODS: A description model for Data-as-a-Service,” in *2012 IEEE 26th International Conference on Advanced Information Networking and Applications*, Mar. 2012. doi: 10.1109/AINA.2012.91. ISSN 1550-445X pp. 605–612. [Online]. Available: http://dx.doi.org/10.1109/AINA.2012.91

[26] J. Gantz and D. Reinsel, “Extracting value from chaos,” *IDC iview*, vol. 1142, no. 2011, pp. 1–12, 2011. [Online]. Available: https://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf

[27] M. D. Assunção, R. N. Calheiros, S. Bianchi, M. A. Netto, and R. Buyya, “Big data computing and clouds: Trends and future directions,” *Journal of Parallel and Distributed Computing*, vol. 79-80, pp. 3–15, 2015. doi: 10.1016/j.jpdc.2014.08.003 Special Issue on Scalable Systems for Big Data Management and Analytics. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0743731514001452

[28] W. Lam, L. Liu, S. Prasad, A. Rajaraman, Z. Vacheri, and A. Doan, “Muppet: MapReduce-style processing of fast data,” *Proc. VLDB Endow.*, vol. 5, no. 12, pp. 1814–1825, Aug. 2012. doi: 10.14778/2367502.2367520. [Online]. Available: http://dx.doi.org/10.14778/2367502.2367520

[29] Z. Zheng, J. Zhu, and M. R. Lyu, “Service-generated Big Data and Big Data-as-a-Service: An overview,” in *2013 IEEE International Congress on Big Data*, Jun. 2013. doi: 10.1109/BigData.Congress.2013.60. ISSN 2379-7703 pp. 403–410. [Online]. Available: http://dx.doi.org/10.1109/BigData.Congress.2013.60

[30] OpenCrowd, “Cloud taxonomy,” http://cloudtaxonomy.opencrowd.com/ [cit. June 12, 2017], Jun. 2017.

[31] W. Heinrichs, “Design management - do it anywhere,” *Electronics Systems and Software*, vol. 3, no. 4, pp. 30–33, Aug. 2005. doi: 10.1049/ess:20050405. [Online]. Available: http://dx.doi.org/10.1049/ess:20050405

[32] X. Xu, “From cloud computing to cloud manufacturing,” *Robotics and Computer-Integrated Manufacturing*, vol. 28, no. 1, pp. 75–86, 2012. doi: 10.1016/j.rcim.2011.07.002. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0736584511000949

[33] M. W. Glowik, L. Mentuccia, and M. Tamietti, “A new era for the automotive industry: How cloud computing will enable automotive companies to change the game,” https://www.accenture.com/t20150914T170053__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Industries_18/Accenture-Cloud-Automative-PoV.pdf [cit. June 12, 2017], 2014.

[34] B. P. Rimal, A. Jukan, D. Katsaros, and Y. Goeleven, “Architectural requirements for cloud computing systems: An enterprise cloud approach,” *Journal of Grid Computing*, vol. 9, no. 1, pp. 3–26, 2011. doi: 10.1007/s10723-010-9171-y. [Online]. Available: http://dx.doi.org/10.1007/s10723-010-9171-y

[35] P. Fingar, “Extreme competition: Cloud oriented business architecture,” *Business Process Trends*, Jun. 2009. [Online]. Available: http://www.bptrends.com/publicationfiles/ONE%2006-09-COL-Extreme%20Competition-Cloud%20Oriented%20Arch-Fingar-final.pdf

[36] A. Vakali, D. Katsaros, K. Stamos, Y. Manolopoulos, A. Sidiropoulos, and G. Pallis, “CDNs content outsourcing via generalized communities,” *IEEE Transactions on Knowledge & Data Engineering*, vol. 21, pp. 137–151, 2008. doi: 10.1109/TKDE.2008.92. [Online]. Available: http://dx.doi.org/10.1109/TKDE.2008.92

[37] M. Baily and J. Manyika, “Is manufacturing’cool’again,” *McKinsey Global Institute*, Jan. 2013. [Online]. Available: http://www.mckinsey.com/mgi/overview/in-the-news/is-manufacturing-cool-again

[38] S. Jain and G. Shao, “Virtual factory revisited for manufacturing data analytics,” in *Proceedings of the 2014 Winter Simulation Conference*, ser. WSC ’14. Piscataway, NJ, USA: IEEE Press, 2014, pp. 887–898. [Online]. Available: http://dl.acm.org/citation.cfm?id=2693848.2693966

[39] J. Lee, E. Lapira, B. Bagheri, and H. an Kao, “Recent advances and trends in predictive manufacturing systems in Big Data environment,” *Manufacturing Letters*, vol. 1, no. 1, pp. 38–41, 2013. doi: 10.1016/j.mfglet.2013.09.005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2213846313000114

[40] J. Lee, B. Bagheri, and H.-A. Kao, “A cyber-physical systems architecture for Industry 4.0-based manufacturing systems,” *Manufacturing Letters*, vol. 3, pp. 18–23, 2015. doi: 10.1016/j.mfglet.2014.12.001. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S221384631400025X

[41] G. Adamson, L. Wang, M. Holm, and P. Moore, “Cloud manufacturing – a critical review of recent development and future trends,” *International Journal of Computer Integrated Manufacturing*, vol. 30, no. 4-5, pp. 347–380, 2017. doi: 10.1080/0951192X.2015.1031704. [Online]. Available: http://dx.doi.org/10.1080/0951192X.2015.1031704

[42] K. Walter, "Final report summary – MANUCLOUD (distributed cloud product specification and supply chain manufacturing execution infrastructure)," European Commission, Germany, FP7-NMP Project Report Summary 260142, 2014. [Online]. Available: http://cordis.europa.eu/result/rcn/59193_en.html

[43] "Diversity (cloud manufacturing and social software based context sensitive product-service engineering environment for globally distributed enterprise)," https://www.diversity-project.eu/ [cit. June 12, 2017], 2015.

[44] "H2020 CREMA project: Providing cloud-based rapid elastic manufacturing based on the xaas and cloud model," http://www.crema-project.eu/Cloud-Manufacturing/ [cit. June 12, 2017], 2015.

[45] "Sustainable manufacturing adaptive services with cloud architectures for enterprises," http://fp7smarter.eu/ [cit. June 12, 2017], 2017.

[46] "cloudSME: Simulation for manufacturing & engineering," http://www.cloudsme-project.eu/ [cit. June 12, 2017], 2016.

[47] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, Apr. 2010. doi: 10.1145/1721654.1721672. [Online]. Available: http://doi.acm.org/10.1145/1721654.1721672

[48] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing – the business perspective," *Decision Support Systems*, vol. 51, no. 1, pp. 176–189, 2011. doi: https://doi.org/10.1016/j.dss.2010.12.006. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167923610002393

[49] G. Booch, "The accidental architecture," *IEEE Software*, vol. 23, no. 3, pp. 9–11, May 2006. doi: 10.1109/MS.2006.86. [Online]. Available: http://dx.doi.org/10.1109/MS.2006.86

[50] Y. Yusuf, M. Sarhadi, and A. Gunasekaran, "Agile manufacturing: The drivers, concepts and attributes," *International Journal of Production Economics*, vol. 62, no. 1-2, pp. 33–43, 1999. doi: 10.1016/S0925-5273(98)00219-9. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0925527398002199

[51] "GitLab.com database incident – 2017/01/31," https://docs.google.com/document/d/1GCK53YDcBWQveod9kfzW-VCxIABGiryG7_z_6jHdVik/pub [cit. June 12, 2017], Feb. 2017.

[52] B. Johnson, "Cloud computing is a trap, warns GNU founder Richard Stallman," *The Guardian*, Sep. 2008. [Online]. Available: https://www.theguardian.com/technology/2008/sep/29/cloud.computing.richard.stallman

[53] J. Heiser and M. Nicolett, "Assessing the security risks of cloud computing," Gartner, Tech. Rep. G00157782, Jun. 2008. [Online]. Available: https://www.gartner.com/doc/685308/assessing-security-risks-cloud-computing

[54] J. Brodkin, "Gartner: Seven cloud-computing security risks," *Network World*, Jul. 2008. [Online]. Available: http://www.networkworld.com/article/2281535/data-center/gartner--seven-cloud-computing-security-risks.html

[55] M. Qiu, W. Gao, M. Chen, J. W. Niu, and L. Zhang, “Energy efficient security algorithm for power grid wide area monitoring system,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 715–723, Dec. 2011. doi: 10.1109/TSG.2011.2160298. [Online]. Available: http://dx.doi.org/10.1109/TSG.2011.2160298

[56] M. Qiu, H. Su, M. Chen, Z. Ming, and L. T. Yang, “Balance of security strength and energy for a PMU monitoring system in smart grid,” *IEEE Communications Magazine*, vol. 50, no. 5, pp. 142–149, May 2012. doi: 10.1109/MCOM.2012.6194395. [Online]. Available: http://dx.doi.org/10.1109/MCOM.2012.6194395

[57] M. Dayarathna, “Comparing 11 IoT development platforms,” https://dzone.com/articles/iot-software-platform-comparison [cit. July 3, 2017], Feb. 2016.

[58] Amazon Web Services, “AWS IoT,” https://aws.amazon.com/iot-platform/how-it-works/ [cit. July 3, 2017], 2017.

[59] ——, “What is AWS IoT?” https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html [cit. July 5, 2017], 2017.

[60] IBM, “Bluemix docs / internet of things platform,” https://console.bluemix.net/docs/services/IoT/index.html [cit. July 5, 2017], 2017.

[61] ——, “The architect’s guide to Bluemix Local,” https://www.ibm.com/cloud-computing/bluemix/sites/default/files/assets/docs/the-architects-guide-to-bluemix-local_0_0.pdf [cit. July 5, 2017], 2017.

[62] O. Bloch, “Developer’s introduction to Azure IoT,” https://azure.microsoft.com/blog/developer-s-introduction-to-azure-iot/ [cit. July 6, 2017], Mar. 2016.

[63] S. Balasubramanian, “Announcing Azure Stream Analytics on edge devices (preview),” https://azure.microsoft.com/en-us/blog/announcing-azure-stream-analytics-on-edge-devices-preview/ [cit. July 6, 2017], Apr. 2017.

[64] S. George, “Microsoft Azure IoT Edge – extending cloud intelligence to edge devices,” https://blogs.microsoft.com/iot/2017/05/10/microsoft-azure-iot-edge-extending-cloud-intelligence-to-edge-devices/ [cit. July 6, 2017], May 2017.

[65] Google, “Google Cloud IoT,” https://cloud.google.com/solutions/iot/ [cit. July 3, 2017], 2017.

[66] ——, “Overview of internet of things,” https://cloud.google.com/solutions/iot-overview [cit. July 7, 2017], 2017.

[67] ——, “Designing a connected vehicle platform on Cloud IoT Core,” https://cloud.google.com/solutions/designing-connected-vehicle-platform [cit. July 7, 2017], 2017.

[68] SAP, “SAP Cloud Platform for the internet of things,” https://www.sap.com/products/iot-platform-cloud.html [cit. July 3, 2017], 2017.

[69] ——, “SAP Cloud Platform Internet of Things service,” https://help.hana.ondemand.com/iot/frameset.htm [cit. July 7, 2017], 2017.

[70] W. Toll, “Top 49 tools for the internet of things,” https://blog.profitbricks.com/top-49-tools-internet-of-things/ [cit. July 3, 2017], Jul. 2014.

[71] mnubo, “Welcome to SmartObjects documentation!” https://smartobjects.mnubo.com/apps/doc/ [cit. July 7, 2017], 2017.

[72] ThingWorx, “ThingWorx studio,” https://s3.amazonaws.com/tpg-thingworx/files/uploads/20161114135055/DS_thingworx-studio_J07272_EN.pdf [cit. July 4, 2017].

[73] “Securing the internet of things: Seven steps to minimize IoT risk in the cloud,” https://www.ptc.com/-/media/Files/PDFs/Services/PTC_IoT_CloudSecurity_WP.ashx [cit. July 4, 2017], Jan. 2016.

[74] “Providing secure connected products,” https://www.thingworx.com/wp-content/uploads/2016/05/WP_thingworx_providing-secure-connected-products-whitepaper_J5194_EN.pdf [cit. July 4, 2017], Apr. 2015.

[75] “MindSphere – industry mall,” https://mall.industry.siemens.com/mall/en/de/Catalog/Products/10011477 [cit. July 2, 2017], 2016.

[76] Siemens AG, “MindSphere with MindConnect Nano and MindConnect IoT2040 – getting started,” https://support.industry.siemens.com/cs/document/109483499, Mar. 2017.

[77] SAP SE, “Security in SAP Cloud Platform: Trust matters,” https://assets.cdn.sap.com/sapcom/docs/2017/05/a470d0b2-b87c-0010-82c7-eda71af511fa.pdf, May 2017.

[78] Cloud Foundry Foundation, “Cloud Foundry documentation,” https://docs.cloudfoundry.org/ [cit. June 29, 2017], 2017.

[79] “Predix architecture and services, updated 11/28/2016,” General Electric Company, Tech. Rep., Nov. 2016. [Online]. Available: https://d154rjc49kgakj.cloudfront.net/GE_Predix_Architecture_and_Services-20161128.pdf

[80] OASIS, “AMQP – advanced message queuing protocol,” https://www.amqp.org/ [cit. August 16, 2017], 2017.

[81] C. Vasters, “Introduction to AMQP 1.0: AMQP foundations,” http://1drv.ms/1KVIJ1X [cit. August 16, 2017], Oct. 2015.

[82] Pearson Education Limited, “Longman dictionary of contemporary english online,” http://www.ldoceonline.com/ [cit. August 16, 2017], 2017.

[83] Gartner, “IT glossary,” https://www.gartner.com/it-glossary/ [cit. August 16, 2017], 2017.

[84] OMG, “Object management group – business process model and notation,” http://www.bpmn.org/ [cit. August 16, 2017], 2017.

[85] “Jericho Forum Commandments, version 1.2,” The Open Group Jericho Forum, Tech. Rep. W124, 2007. [Online]. Available: https://www2.opengroup.org/ogsys/catalog/W124

[86] Y. Altintas, *Computer Numerical Control.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 249–252. ISBN 978-3-642-20617-7. [Online]. Available: https://doi.org/10.1007/978-3-642-20617-7_6524

[87] L. Monostori, "Cyber-physical production systems: Roots, expectations and R&D challenges," *Procedia CIRP*, vol. 17, pp. 9–13, 2014. doi: http://dx.doi.org/10.1016/j.procir.2014.03.115 Variety Management in Manufacturing. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2212827114003497

[88] A. P. Noble, R. Kopaee, A. Melek, and N. Nandy, "Data leak prevention," ISACA, Tech. Rep., Sep. 2010. [Online]. Available: http://www.isaca.org/Groups/Professional-English/security-trend/GroupDocuments/DLP-WP-14Sept2010-Research.pdf

[89] J. Karnon, J. Stahl, A. Brennan, J. J. Caro, J. Mar, and J. Möller, "Modeling using discrete event simulation," *Medical Decision Making*, vol. 32, no. 5, pp. 701–711, 2012. doi: 10.1177/0272989X12455462. [Online]. Available: http://dx.doi.org/10.1177/0272989X12455462

[90] "eXtensible Access Control Markup Language (XACML) version 2.0," OASIS, Tech. Rep., Feb. 2005. [Online]. Available: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[91] T. Bray, J. Paoli, C. M. Sperberg-McQueen, E. Maler, F. Yergeau, and J. Cowan, "Extensible markup language (XML) 1.1 (second edition)," W3C, W3C Recommendation, 2006. [Online]. Available: http://www.w3.org/TR/2006/REC-xml11-20060816

[92] J. Postel and J. K. Reynolds, "File transfer protocol," RFC 959, IETF, Oct. 1985. [Online]. Available: https://tools.ietf.org/html/rfc959

[93] R. Fielding and J. Reschke, "Hypertext transfer protocol (HTTP/1.1): Message syntax and routing," RFC 7230, IETF, Jun. 2014. [Online]. Available: https://tools.ietf.org/html/rfc7230

[94] E. Rescorla, "HTTP over TLS," RFC 2818, IETF, May 2000. [Online]. Available: https://tools.ietf.org/html/rfc2818

[95] C. Emig, F. Brandt, S. Kreuzer, and S. Abeck, *Identity as a Service – Towards a Service-Oriented Identity Management Architecture.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 1–8. ISBN 978-3-540-73530-4. [Online]. Available: https://doi.org/10.1007/978-3-540-73530-4_1

[96] S. Bhardwaj, L. Jain, and S. Jain, "Cloud computing: A study of infrastructure as a service (IAAS)," *International Journal of engineering and information Technology*, vol. 2, no. 1, pp. 60–63, 2010.

[97] R. H. Weber and R. Weber, *Introduction.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 1–22. ISBN 978-3-642-11710-7. [Online]. Available: https://doi.org/10.1007/978-3-642-11710-7_1

[98] J. Postel, "Internet protocol," RFC 791, IETF, Sep. 1981. [Online]. Available: https://tools.ietf.org/html/rfc791

[99] AXELOS, “What is ITIL best practice?” https://www.axelos.com/best-practice-solutions/itil/what-is-itil [cit. August 16, 2017], 2017.

[100] JSON, “Introducing JSON,” http://json.org/ [cit. August 16, 2017], 2017.

[101] J. Sermersheim, “Lightweight directory access protocol (LDAP): The protocol,” RFC 4511, IETF, Jun. 2006. [Online]. Available: https://tools.ietf.org/html/rfc4511

[102] H. Schleifenbaum, J.-Y. Uam, G. Schuh, and C. Hinke, “Turbulence in production systems – fluid dynamics and its contributions to production theory,” in *Proceedings of the World Congress on Engineering and Computer Science*, vol. 2, San Francisco, USA, Oct. 2009. ISBN 978-988-18210-2-7. [Online]. Available: http://www.iaeng.org/publication/WCECS2009/WCECS2009_pp1140-1145.pdf

[103] U. Rauschecker, M. Meier, R. Muckenhirn, A. L. K. Yip, A. P. Jagadeesan, and J. Corney, “Cloud-based manufacturing-as-a-service environment for customized products,” in *eChallenges e-2011 Conference Proceedings*, P. Cunningham and M. Cunningham, Eds. IIMC International Information Management Corporation, 2011. [Online]. Available: http://strathprints.strath.ac.uk/38573/

[104] S. H. Chung and C. A. Snyder, “ERP adoption: a technological evolution approach,” *International Journal of Agile Management Systems*, vol. 2, no. 1, pp. 24–32, 2000. doi: 10.1108/14654650010312570. [Online]. Available: https://doi.org/10.1108/14654650010312570

[105] J. Dean and S. Ghemawat, “MapReduce: Simplified data processing on large clusters,” *Commun. ACM*, vol. 51, no. 1, pp. 107–113, Jan. 2008. doi: 10.1145/1327452.1327492. [Online]. Available: http://doi.acm.org/10.1145/1327452.1327492

[106] “MQTT version 3.1.1,” OASIS, Tech. Rep., Oct. 2014. [Online]. Available: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.pdf

[107] MODBUS, “MODBUS application protocol specification v1.1b3,” Modbus Organization, Apr. 2012. [Online]. Available: http://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf

[108] D. K. Barry, “Network as a service (NaaS),” http://www.service-architecture.com/articles/cloud-computing/network_as_a_service_naas.html [cit. August 16, 2017], Barry & Associates, 2017.

[109] D. Hardt, “The OAuth 2.0 authorization framework,” RFC 6749, IETF, Oct. 2012. [Online]. Available: https://tools.ietf.org/html/rfc6749

[110] OPC Foundation, “Unified architecture,” https://opcfoundation.org/about/opc-technologies/opc-ua/ [cit. August 16, 2017], 2017.

[111] SPI, “Open MPI: Open source high performance computing,” https://www.open-mpi.org/ [cit. August 16, 2017], Software in the Public Interest, 2017.

[112] L. Youseff, M. Butrico, and D. D. Silva, “Toward a unified ontology of cloud computing,” in *2008 Grid Computing Environments Workshop*, Nov. 2008. doi: 10.1109/GCE.2008.4738443. ISSN 2152-1085 pp. 1–10. [Online]. Available: https://doi.org/10.1109/GCE.2008.4738443

[113] N. M. Vichare and M. G. Pecht, “Prognostics and health management of electronics,” *IEEE Transactions on Components and Packaging Technologies*, vol. 29, no. 1, pp. 222–229, Mar. 2006. doi: 10.1109/TCAPT.2006.870387. [Online]. Available: https://doi.org/10.1109/TCAPT.2006.870387

[114] FDA, “Radio frequency identification (RFID),” https://www.fda.gov/Radiation-EmittingProducts/RadiationSafety/ElectromagneticCompatibilityEMC/ucm116647.htm [cit. August 16, 2017], U.S. Food and Drug Administration, 2017.

[115] R. T. Fielding, “Architectural styles and the design of network-based software architectures,” Ph.D. dissertation, University of California, Irvine. ISBN 0-599-87118-0 2000. [Online]. Available: http://www.ics.uci.edu/~fielding/pubs/dissertation/fielding_dissertation.pdf

[116] D. Simon, B. Espiau, E. Castillo, and K. Kapellos, “Computer-aided design of a generic robot controller handling reactivity and real-time control issues,” *IEEE Transactions on Control Systems Technology*, vol. 1, no. 4, pp. 213–229, Dec. 1993. doi: 10.1109/87.260267. [Online]. Available: https://doi.org/10.1109/87.260267

[117] P. K. A. Freier, P. Karlton, “The secure sockets layer (SSL) protocol version 3.0,” RFC 6101, IETF, Aug. 2011. [Online]. Available: https://tools.ietf.org/html/rfc6101

[118] OASIS, “SAML XML.org,” http://saml.xml.org/ [cit. August 16, 2017], 2017.

[119] AXELOS, “ITIL glossary and abbreviations english v.1.0,” https://www.axelos.com/Corporate/media/Files/Glossaries/ITIL_2011_Glossary_GB-v1-0.pdf [cit. August 16, 2017], 2011.

[120] P. Hall, “Creative cities and economic development,” *Urban Studies*, vol. 37, no. 4, pp. 639–649, 2000. doi: 10.1080/00420980050003946. [Online]. Available: http://dx.doi.org/10.1080/00420980050003946

[121] A. Cocchia, *Smart and Digital City: A Systematic Literature Review.* Cham: Springer International Publishing, 2014, pp. 13–43. ISBN 978-3-319-06160-3. [Online]. Available: https://doi.org/10.1007/978-3-319-06160-3_2

[122] ABB, “What is a smart grid?” http://new.abb.com/smartgrids/what-is-a-smart-grid [cit. August 16, 2017], 2017.

[123] J. Wu, L. Ping, X. Ge, Y. Wang, and J. Fu, “Cloud storage as the infrastructure of cloud computing,” in *2010 International Conference on Intelligent Computing and Cognitive Informatics*, Jun. 2010. doi: 10.1109/ICICCI.2010.119 pp. 380–383.

[124] IETF, “SCIM: System for cross-domain identity management,” http://www.simplecloud.info/ [cit. August 16, 2017], IETF, 2017.

[125] E. R. T. Dierks, “The transport layer security (TLS) protocol version 1.2,” RFC 5246, IETF, Aug. 2008. [Online]. Available: https://tools.ietf.org/html/rfc5246

[126] S. Jain, N. F. Choong, K. M. Aye, and M. Luo, “Virtual factory: an integrated approach to manufacturing systems modeling,” *International Journal of Operations & Production Management*, vol. 21, no. 5/6, pp. 594–608, 2001. doi: 10.1108/01443570110390354. [Online]. Available: https://doi.org/10.1108/01443570110390354

[127] Kaazing, “websocket.org,” https://www.websocket.org/ [cit. August 16, 2017], 2017.

[128] I. Fette and A. Melnikov, “The WebSocket protocol,” RFC 6455, IETF, Dec. 2011. [Online]. Available: https://tools.ietf.org/html/rfc6455

[129] M. Zima, M. Larsson, P. Korba, C. Rehtanz, and G. Andersson, “Design aspects for wide-area monitoring and control systems,” *Proceedings of the IEEE*, vol. 93, no. 5, pp. 980–996, May 2005. doi: 10.1109/JPROC.2005.846336. [Online]. Available: https://doi.org/10.1109/JPROC.2005.846336

[130] M. Smith, “Workforce performance management: Efficiency and effectiveness,” *InformationWeek*, Nov. 2004. [Online]. Available: http://www.informationweek.com/d/d-id/1028711

Glossary

Advanced Message Queuing Protocol over TLS/SSL (AMQPS) An open protocol for passing business messages between various IT applications or systems in organizations with secure communication over Transport Layer Security (TLS)/Secure Sockets Layer (SSL). The protocol is described in ISO/IEC 19464:2014. It defines a middleware for standardised and reliable exchange of business messages between two parties. The messages are delivered by various means including classic message brokers (the parties are able to publish messages of particular types and to subscribe to the message types) and peer-to-peer exchange (the parties are able to send messages to particular receivers only). The protocol is suitable for seamless integration of various systems with both legacy and new applications, databases and other shared resources, including the systems and the resources running in cloud. [80, 81]. 41, 77

application programming interface (API) A set of computer codes that make it possible for different types of software to communicate with each other and exchange data. [82]. 5, 39, 65, 77

augmented reality (AR) A situation in which computer-generated information, images, etc. are combined with things in the real world or images of real things. [82]. 45, 77

Big data Data that can be characterised by five Vs: variety, velocity, volume, veracity, and value. Variety represents the data types, velocity refers to the rate at which the data is produced and processed, and volume defines the amount of data. Veracity refers to how much the data can be trusted given the reliability of its source, whereas value corresponds the monetary worth that a company can derive from employing Big data computing. [27]. 11, 15, 16, 23, 28, 29, 38–41, 43, 44, 47, 51, 54, 55, 57–61, 66, 70

business activity monitoring (BAM) Processes and technologies that enhance situation awareness and enable analysis of critical business performance indicators based on real-time data. It is used to improve the speed and effectiveness of business operations by keeping track of what is happening and making issues visible quickly. This concept can be implemented through many different kinds of software tools; those aimed solely at BAM are called BAM platform products. [83]. 21, 77

Business Process Management (BPM) A discipline that uses various methods to discover, model, analyse, measure, improve, and optimize business processes. A business process coordinates the behaviour of people, systems, information, and things to produce business outcomes in support of a business strategy. Processes can be structured and repeatable or unstructured and variable. Though not required, technologies are often used with BPM. BPM is key to align IT and operational technology investments to business strategy. [83]. 19, 21, 59, 77

Business Process Modelling Notation (BPMN) A graphical notation that depicts the steps in a business process, i.e., the end to end flow of a business process. The notation has been specifically designed to coordinate the sequence of processes and the messages that flow between different process participants in a related set of activities. It provides businesses with the capability of understanding their internal business procedures in the graphical notation and gives organizations the ability to communicate these procedures in a standard manner. Furthermore, the graphical notation facilitates the understanding of the performance collaborations and business transactions between the organizations. This ensures that businesses will understand themselves and participants in their business and enables organizations to adjust to new internal and business-to-business circumstances quickly. [84]. 55, 77

cloud computing A style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies. It is a distributed and on-demand concept of computing that aims to solve well-known problems of IT systems, such as high maintenance and IT infrastructure costs, low scalability and agility, problematic outsourcing, and others. [83]. 1–4, 6–12, 14–16, 19, 20, 22, 23, 26–33, 35, 37–42, 44, 45, 48–50, 53, 54, 59–61

Cloud Cube Model (CCM) A model of cloud computing proposed by Jericho Forum to identify four criteria to differentiate cloud formations from each other and the manner of their provision. In the model, the Jericho Forum objectives related to cloud computing are focused on enabling secure business collaboration in the appropriate cloud formations best suited to the business needs. There are several types of cloud, and each type has features which need to be correctly understood to inform sound business decision-making on which type is best suited to the requirements that business is looking for. The model presents the different types of cloud, highlighting the key characteristics in each type. It includes key questions that prospective cloud users need to ask their cloud service providers to provide adequate assurance that they are securely collaboratively enabled and compliant with applicable regulations. Cloud computing is the ultimate de-perimeterised environment. It has no boundaries. While private clouds may purport to constrain access to their program platforms and applications, and to the data on which they operate, the physical locations of the servers and computational resources they provide are unknown. Cloud is truly a boundary-less environment requiring information security which satisfies the criteria set out in the Jericho Forum Commandments. [7, 85]. iii, 6, 38, 77

cloud manufacturing (CMfg) A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable manufacturing resources (e.g., manufacturing software tools, manufacturing equipment, and manufacturing capabilities) that can be rapidly provisioned and released with minimal management effort or service provider interaction. In cloud manufacturing, distributed resources are encapsulated into cloud services and managed in a centralized way. Clients can use cloud services according to their requirements. Cloud users can request services ranging from product design, manufacturing, testing, management, and all other stages of a product life cycle. [32]. 19, 25, 37, 59, 61, 77

computer numeric control (CNC) The digital control of machine tool units that consist of series of integrated mechanical actuators, electrical or electro-hydraulic servomotors, power amplifiers, position and velocity sensors, and a dedicated computer running under a real-time operating system. [86]. 12, 77

content distribution network (CDN) An overlay computer network across Internet providing a scalable and cost-effective mechanism for accelerating the delivery of the Web content. The network consists of a set of surrogate servers (distributed around the world), routers, and network elements. Surrogate servers are the key elements in a CDN, acting as proxy caches that serve directly cached content to clients. They store copies of identical content, such that clients' requests are satisfied by the most appropriate site. Once a client requests for content on an origin server (managed by a CDN), his request is directed to the appropriate CDN's surrogate server. This results in an improvement to both the response time (the requested content is nearest to the client) and the system throughput (the workload is distributed to several servers). [36]. 21, 77

customer relationship management (CRM) A business strategy that optimizes revenue and profitability while promoting customer satisfaction and loyalty. CRM technologies enable strategy, and identify and manage customer relationships, in person or virtually. CRM software provides functionality to companies in four segments: sales, marketing, customer service and digital commerce. [83]. 19, 77

cyber-physical production system (CPPS) A system of collaborating computational entities which are in intensive connection with the surrounding physical world of manufacturing and its on-going processes, providing and using, at the same time, data-accessing and data-processing services. Such systems consist of autonomous and co-operative elements and sub-systems that are getting into connection with each other in situation dependent ways, on and across all levels of production, from processes through machines up to production and logistics networks. [87]. 12, 77

Data as a Service (DaaS) A type of cloud computing services that provide data on demand. Such service typically exposes its provided data to consumers through application programming interfaces (APIs), either for the consumer to download or query data from different data assets. By using these services, consumers do not need to fetch and store giant data assets and search for the required information in the data asset. Instead, they simply find a suitable service that provides the data asset having the desired information and call the corresponding APIs to retrieve the data. [25]. iii, 14, 27, 37, 59, 78

data loss prevention (DLP) A suite of technologies aimed at stemming the loss of sensitive information that occurs in enterprises across the globe. By focusing on the location, classification and monitoring of information at rest, in use and in motion, this solution can go far in helping an enterprise get a handle on what information it has, and in stopping the numerous leaks of information that occur each day. DLP is not a plug-and-play solution. The successful implementation of this technology requires significant preparation and diligent ongoing maintenance. Enterprises seeking to integrate and implement DLP should be prepared for a significant effort that, if done correctly, can greatly reduce risk to the organization. Those implementing the solution must take a strategic approach that addresses risks, impacts and mitigation steps, along with appropriate governance and assurance measures. [88]. 34, 78

database and file activity monitoring (DAM/FAM) A suite of tools that can be used to support the ability to identify and report on fraudulent, illegal or other undesirable behaviour, with minimal impact on user operations and productivity. The tools, which have evolved from basic analysis of user activity in and around relational database management systems (and file storages) to encompass a more comprehensive set of capabilities, such as discovery and classification, vulnerability management, application-level analysis, intrusion prevention, support for unstructured data security, identity and access management integration, and risk management support. [83]. 34, 78

Design Anywhere, Manufacture Anywhere (DAMA) A manufacturing philosophy enabling companies to move their design and manufacturing facilities at short notice to respond to changes in the market, to have the flexibility to expand and contract these to fit with demand cycles, and to add new design centres and plants that can be quickly integrated into the business process as a whole. This approach demands the ability to exchange design data across sites and to harmonise design tools, components and manufacturing. [31]. 19, 78

digital rights management (DRM) Trusted exchange of digital information over the Internet whereby the user is granted only the privileges that the document sender allows. [83]. 34, 78

discrete event simulation (DES) A form of computer-based modelling that provides an intuitive and flexible approach to representing complex systems (with chronologically non-decreasing sequence of event occurrences). DES was developed in the 1960s in industrial engineering and operations research to help analyse and improve industrial and business processes. The term discrete refers to the fact that DES moves forward in time at discrete intervals (i.e., the model jumps from the time of one event to the time of the next) and that the events are discrete (mutually exclusive). These factors give DES the flexibility and efficiency to be used over a very wide range of problems. The core concepts of DES are entities, attributes, events, resources, queues, and time. Entities are objects that have attributes, experience events, consume resources, and enter queues, over time. Attributes are features specific to each entity that allow it to carry information. Events are broadly defined as things that can happen to an entity or the environment. A resource is an object that provides a service to an entity. If a resource is "occupied" when an entity needs it, then that entity must wait, forming a queue. And finally, an explicit simulation clock (initiated at the start of the model run) keeps track of time. [89]. 24, 78

enterprise resource planning (ERP) The ability to deliver an integrated suite of business applications. ERP tools share a common process and data model, covering broad and deep operational end-to-end processes, such as those found in finance, HR, distribution, manufacturing, service and the supply chain. [83]. 12, 19, 78

eXtensible Access Control Markup Language (XACML) A core Extensible Markup Language (XML) schema OASIS Standard for representing authorization and entitlement policies which serves as a common language for expressing security policy. If implemented throughout an enterprise, the common policy language allows the enterprise to manage the enforcement of all the elements of its security policy in all the components of its information systems. Managing security policy may include some or all of the following steps: writing, reviewing, testing, approving, issuing, combining, analysing, modifying, withdrawing, retrieving and enforcing policy. [90]. 56, 80

Extensible Markup Language (XML) A markup language for a text documents in a format that is both human- and machine-readable. The XML, which was originally designed to meet the challenges of large-scale electronic publishing, is also playing an increasingly important role in the exchange of a wide variety of data on the Web and elsewhere. XML documents are made up of storage units called entities, which contain either parsed or unparsed data. Parsed data is made up of characters, some of which form character data, and some of which form markup. Markup encodes a description of the document's storage layout and logical structure. XML provides a mechanism to impose constraints on the storage layout and logical structure. [91]. 66, 80

Fast data Big data with focus on velocity, for example, high-speed real-time and near-real-time data streams. Prime examples of Fast data include sensor data streams, real-time stock market data, and social-media feeds. The Fast data often must be processed with minimal latency and high scalability. [28]. 15, 51, 55, 59

File Transfer Protocol (FTP) A network application protocol for the file transfer between a client and server on a computer network. The objectives of FTP are to promote sharing of files (computer programs and/or data), to encourage indirect or implicit (via programs) use of remote computers, to shield a user from variations in file storage systems among hosts, and to transfer data reliably and efficiently. FTP, though usable directly by a user at a terminal, is designed mainly for use by programs. [92]. 55, 78

grid computing A method for applying large numbers of resources, usually large amounts of processing capacity, to a single (non-interactive) task, by applying resources from more than one system. A grid is a collection of resources that is coordinated to enable the resources to solve a common problem. A computing grid harnesses multiple computers from several owners to run one very large application problem. [83]. 2, 9

Hypertext Transfer Protocol (HTTP) A stateless application-level request/response protocol that uses extensible semantics and self-descriptive message payloads for flexible interaction with network-based hypertext information systems. It is designed as a generic interface protocol for information systems, to hide the details of how a service is implemented by presenting a uniform interface to clients that is independent of the types of resources provided. Likewise, servers do not need to be aware of each client's purpose: an HTTP request can be considered in isolation rather than being associated with a specific type of client or a predetermined sequence of application steps. The result is a protocol that can be used effectively in many different contexts and for which implementations can evolve independently over time. HTTP is also designed for use as an intermediation protocol for translating communication to and from non-HTTP information systems. HTTP proxies and gateways can provide access to alternative information services by translating their diverse protocols into a hypertext format that can be viewed and manipulated by clients in the same way as HTTP services. [93]. 41, 67, 78

Hypertext Transfer Protocol over Transport Layer Security (HTTPS) A secure and stateless application-level request/response protocol that uses extensible semantics and self-descriptive message payloads for flexible interaction with network-based hypertext information systems. The protocol consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by TLS. [94, 93]. 44, 78

Identity as a Service (IdaaS) A cloud-based service that provides identity and access management functions. It allows to verify authorization for an application (e.g., other cloud services) usage at runtime by enabling access control. Access control is based on two prerequisites. First, an authentication process checking any possible credentials has to be passed. This can be done by direct communication of a user and an IdaaS service, without participation of the application. Second, an authorization verification process is needed which checks if permission has been granted. This can be done by direct communication of the application and the IdaaS service, without participation of the user. The functionality of both (i.e., authentication and authorization verification) as well as the identity management functionality is encapsulated in the IdaaS service and available to applications, users, and other cloud services. [95]. 5, 78

information technology (IT) The study or use of electronic processes for gathering and storing information and making it available using computers. [82]. 1, 19, 41, 59, 61, 78

Infrastructure as a Service (IaaS) The delivery of hardware (server, storage and network), and associated software (operating systems virtualization technology, file system), as a service. It is an evolution of traditional hosting that does not require any long term commitment and allows users to provision resources on demand. Unlike Platform as a Service (PaaS) services, the IaaS provider does very little management other than keep the data centre operational and users must deploy and manage the software services themselves just the way they would in their own data centre. [96]. 3, 5, 19, 37, 59, 74, 78

Internet of Things (IoT) An emerging global Internet-based information architecture facilitating the exchange of goods and services. It has the purpose of providing an IT-infrastructure facilitating the exchange of “things” in a secure and reliable manner, i.e., its function is to overcome the gap between objects in the physical world and their representation in information systems. It will serve to increase transparency and enhance the efficiency of global supply chain networks. [97]. 12, 38, 59, 70, 78

Internet Protocol (IP) A low-level communications protocol designed for use in interconnected systems of packet-switched computer communication networks. The protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length IP addresses. It also provides means for fragmentation and reassembly of long datagrams, if necessary, for transmission through “small packet” networks. [98]. 7, 21, 74, 78

IT Infrastructure Library (ITIL) A widely accepted approach to IT Service Management that provides a cohesive set of best practice, drawn from the public and private sectors internationally. ITIL advocates that IT services are aligned to the needs of the business and support its core processes. It provides guidance to organizations and individuals on how to use IT as a tool to facilitate business change, transformation and growth. ITIL is mapped in ISO 20000 Part 11 which recognizes the way that ITIL can be used in order to meet the requirements set out for ISO 20000 certification and the interdependent nature with ITIL. ITIL’s IT Service Management Best Practice is supported by a certification scheme that enables practitioners to demonstrate their abilities in adopting and adapting the framework to address their specific needs. [99]. 27, 78

JavaScript Object Notation (JSON) A lightweight data-interchange text format, easy for humans to read and write and easy for machines to parse and generate. It is based on a subset of the JavaScript Programming Language, however, it is a text format that is completely language independent but uses conventions that are familiar to programmers of the C-family of languages, including C, C++, C#, Java, JavaScript, Perl, Python, and many others. These properties make JSON an ideal data-interchange language. JSON is built on two structures: a collection of name/value pairs and an ordered list of values. The first one is usually, in various languages, realized as an object, record, structure, dictionary, hash table, keyed list, or associative array. The second one is usually realized as an array, vector, list, or sequence. These two are universal data structures. Virtually all modern programming languages support them in one form or another. It makes sense that a data format that is interchangeable with programming languages also be based on these structures. [100]. 56, 78

key performance indicator (KPI) A high-level measure of system output, traffic or other usage, simplified for gathering and review on a weekly, monthly or quarterly basis. Typical examples are bandwidth availability, transactions per second and calls per user. KPIs are often combined with cost measures (e.g., cost per transaction or cost per user) to build key system operating metrics. [83]. 14, 29, 38, 78

Lightweight Directory Access Protocol (LDAP) It is a directory access protocol for distributed directory services. The directory is a collection of open systems cooperating to provide directory services. A directory user, which may be a human or other entity, accesses the directory through a client. The client, on behalf of the directory user, interacts with one or more servers using a directory access protocol such as LDAP. [101]. 47, 79

lot size one A manufacturing where each part of a final product flow constantly throughout the product creation chain as a single unit, so the production can be decomposed and it is flexible in modifications of its individual parts (which is a necessary precondition for on-demand manufacturing where the processes need to be reconfigured on demand). [102]. 12

Manufacturing as a Service (MaaS) It is a paradigm of cloud-based services which are used to envisage a new generation of configurable manufacturing systems. Unlike previous approaches to mass customization (that simply reprogram individual machines to produce specific shapes) the system reported here is intended to enable the customized production of technologically complex products by dynamically configuring a manufacturing supply chain. In order to realize such a system, the resources (i.e., production capabilities) have to be designed to support collaboration throughout the whole production network, including their adaption to customer-specific production. The flexible service composition as well as the appropriate IT services required for its realization show many analogies with common cloud computing approaches. [103]. 24, 37, 79

manufacturing execution system (MES) A system which manages, monitors and synchronizes the execution of real-time, physical processes involved in transforming raw materials into intermediate and/or finished goods. Such systems coordinate this execution of work orders with production scheduling and enterprise-level systems. MES applications also provide feedback on process performance, and support component- and material-level traceability, genealogy, and integration with process history, where required. [83]. 12, 79

manufacturing resource/requirements planning (MRP) The application of information and manufacturing technology, plans and resources to improve the efficiency of a manufacturing enterprise through integration effort. It evolved from material requirements planning, however, contrary to the material requirements planning, it is used not only for planning materials and parts to production, but also for manufacturing plans and schedules. In manufacturing resource planning, all of the lead time elements, shop routing, and process times are assumed to be deterministic. Linking other activities such as purchasing, inventory control and sales is performed in isolated planning and scheduling by simply retrieving, storing, and interchanging data in the system only when needed. [104]. 19, 79

MapReduce A programming model and an associated implementation for processing and generating large datasets (Big data) that is amenable to a broad variety of real-world tasks. Users specify the computation in terms of a map and a reduce function, and the underlying runtime system automatically parallelizes the computation across large-scale clusters of machines, handles machine failures, and schedules inter-machine communication to make efficient use of the network and disks. [105]. 15

Message Queue Telemetry Transport (MQTT) ISO/IEC PRF 20922 standard for a lightweight machine-to-machine (M2M) messaging protocol based on the publisher-subscriber communication model running on top of the TCP/IP protocol. The protocol is light weight, open, simple, and designed so as to be easy to implement. These characteristics make it ideal for use in many situations, including constrained environments such as for communication in M2M and Internet of Things (IoT) contexts where a small code footprint is required and/or network bandwidth is at a premium. The protocol runs over TCP/IP, or over other network protocols that provide ordered, lossless, bi-directional connections. Its features include: use of the publish/subscribe message pattern which provides one-to-many message distribution and decoupling of applications; a messaging transport that is agnostic to the content of the payload; three qualities of service for message delivery (at most once, at least once, and exactly once); a small transport overhead and protocol exchanges minimized to reduce network traffic; a mechanism to notify interested parties when an abnormal disconnection occurs. [106]. 39, 79

Modbus An application-layer messaging protocol which provides client/server communication between devices connected on different types of buses or networks. It is a request/reply protocol which offers services specified by function codes. The function codes are elements of Modbus request/reply protocol data units sent from a client to server devices together with additional information that the server uses to take the action defined by the function code. [107]. 42

Network as a Service (NaaS) A cloud-based service that provides virtualised network infrastructure on demand. It can include flexible and extended virtual private network (VPN), bandwidth on demand, custom routing, multicast protocols, security firewall, intrusions detection and prevention, wide area network, content monitoring and filtering, and antivirus. There is no standard specification as to what is included in NaaS. Implementations vary. [108]. 5, 79

OAuth An open industry-standard protocol to allow secure authorization in a simple and standard method from web, mobile and desktop applications. It enables a third-party application to obtain limited access to a service, either on behalf of a resource owner (an end-user) by orchestrating an approval interaction between the resource owner (the end-user) and the service, or by allowing the third-party application to obtain access on its own behalf. [109]. 44, 56

OPC Unified Architecture (OPC-UA) A platform independent service-oriented architecture that integrates all the functionality of the individual OPC Classic specifications into one extensible framework. While OPC Classic was based on Microsoft Windows technology using the Distributed Component Object Model for the exchange of data between software components, OPC UA is platform independent and available for various hardware platforms and operating systems (traditional computer hardware, cloud-based servers, programmable logic controllers (PLCs), micro-controllers, etc. running Microsoft Windows, Apple OSX, Android, or any distribution of Linux, etc.). OPC UA is functionally equivalent to OPC Classic, yet capable of much more. Moreover, it is firewall-friendly while addressing security concerns by providing a suite of controls such as secure transport, session encryption, message signing, sequenced packets preventing message replay attacks, authentication, user control, and auditing. [110]. 42, 79

Open MPI It is an open source message passing interface implementation (MPI stands for the Message Passing Interface). Open MPI is developed and maintained by a consortium of academic, research, and industry partners for distributed and parallel high performance computing. It is a standardized API typically used for parallel and/or distributed computing. [111]. 2

Platform as a Service (PaaS) A service of the cloud software environment layer (also dubbed the software platform layer). The users of this layer are cloud applications' developers, implementing their applications for and deploying them on the cloud. The providers of the cloud software environments supply the developers with a programming-language-level environment with a set of well-defined APIs to facilitate the interaction between the environments and the cloud applications, as well as to accelerate the deployment and support the scalability needed of those cloud applications. [112]. 3, 4, 19, 37, 59, 68, 79

prognostics and health management (PHM) A method that permits the reliability of a system to be evaluated in its actual life-cycle conditions, to determine the advent of failure, and mitigate the system risks. A considerable body of knowledge exists on prognostics and health management of safety-critical mechanical systems and structures, with research conducted in establishing failure precursors (such as changes in vibration signatures of roller bearings and variations in acoustic levels due to wear) and developing reasoning algorithms. However, this is not the case for electronic systems where degradation in electronics is more difficult to detect and inspect than most mechanical systems and structures, due to the micro- to nanoscale and the complex architecture of most electronic products. [113]. 23, 24, 59, 79

programmable logic controller (PLC) The fundamental building block of factory and process automation. A specially purpose computer, including input/output processing and serial communications, used for executing control programs, especially control logic and complex interlock sequences. PLCs can be embedded in machines or process equipment by original manufacturers, used stand-alone in local control environments or networked in system configurations. [83]. 12, 37, 71, 79

quality of service (QoS) A negotiated contract, such as Service Level Agreement (SLA), between a user and a service provider that renders some degree of performance (e.g., a degree of reliable capacity in the shared network for a service of a network provider). [83]. 11, 79

Radio-frequency Identification (RFID) A wireless system comprised of two components: tags and readers. The reader is a device that has one or more antennas that emit radio waves and receive signals back from the RFID tag. Tags, which use radio waves to communicate their identity and other information to nearby readers, can be passive or active. Passive RFID tags are powered by the reader and do not have a battery. Active RFID tags are powered by batteries. RFID tags can store a range of information from one serial number to several pages of data. Readers can be mobile so that they can be carried by hand, or they can be mounted on a post or overhead. Reader systems can also be built into the architecture of a cabinet, room, or building. [114]. 12, 79

Representational State Transfer (REST) A client-server layered architectural style of web resources utilised often for Web services to access them by a uniform interface in a stateless and cacheable way. The REST style is an abstraction of the architectural elements within a distributed hypermedia system where all data is encapsulated within and hidden by the processing components. REST components communicate by transferring a representation of a resource in a format matching one of an evolving set of standard data types, selected dynamically based on the capabilities or desires of the recipient and the nature of the resource. Any information that can be named can be a resource: a document or image, a temporal service, a collection of other resources, a non-virtual object (e.g., a person), and so on. Whether the representation of a resource is in the same format as the raw source, or is derived from the source, remains hidden behind the interface. [115]. 41, 74, 79

Robot as a Service (RaaS) A cloud-based service that provides the access, monitoring, and control of robots seamlessly integrated into the cloud and operating on demand. A robot is considered to be a mechanical or virtual artificial agent, which, by its appearance or movements, conveys a sense that it has intent or agency of its own. According to RaaS, a robot should be able to act as service provider. A client can deploy new services into a robot, so that the services can be used by this robot and can also be shared with other robots and composed into a new application based on the services available in and outside the robot. Moreover, a robot should be able to act also as both a service broker and a service client. A client, external or a robot, can search and discover applications and services deployed on another robot. [24]. iii, 12, 14, 37, 59, 79

robot controller (RC) A set of hardware and software resources involved in the on-line control of a set of cooperating devices (such as robots and sensors) associated with a control system. [116]. 12, 75, 79

Secure Sockets Layer (SSL) A security protocol that provides communications privacy over the Internet and allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. The protocol is used for encapsulation of various higher level protocols. One such encapsulated protocol, the SSL handshake protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. One advantage of SSL is that it is application protocol independent. A higher level protocol can layer on top of the SSL protocol transparently. The SSL protocol provides connection security that has three basic properties: the connection is private (encryption is used after an initial handshake to define a secret key and then, symmetric cryptography is used for data encryption by this secret key), the peer's identity can be authenticated (using asymmetric, or public key, cryptography), and the connection is reliable (message transport includes a message integrity check using a keyed message authentication code computed by secure hash functions). The protocol is a predecessor of TLS. [117]. 34, 56, 63, 80

Security Assertion Markup Language (SAML) An XML-based framework for creating and exchanging security information, such as user authentication, entitlement, and attribute information, between online partners. SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application. Prior to SAML, there was no XML-based standard that enabled exchange of security information between a security system (such as an authentication authority) and an application that trusts the security system. SAML provides a standard XML representation for specifying this information and interoperable ways to exchange and obtain it. [118]. 44, 79

Service Level Agreement (SLA) An agreement between an IT service provider and a customer. A service level agreement describes the IT service, documents service level targets, and specifies the responsibilities of the IT service provider and the customer. A single agreement may cover multiple IT services or multiple customers. [119]. 30, 53, 71, 80

service-oriented architecture (SOA) A design paradigm and discipline that helps IT meet business demands. Some organizations realize significant benefits using SOA including faster time to market, lower costs, better application consistency and increased agility. SOA reduces redundancy and increases usability, maintainability and value. This produces interoperable, modular systems that are easier to use and maintain. SOA creates simpler and faster systems that increase agility and reduce total cost of ownership. [83]. 14, 80

smart city A city that monitors and integrates conditions of all of its critical infrastructures, including roads, bridges, tunnels, rails, subways, airports, seaports, communications, water, power, even major buildings, can better optimize its resources, plan its preventive maintenance activities, and monitor security aspects while maximizing services to its citizens. [120, 121]. 11, 12

smart grid A power grid system that manages electricity demand in a sustainable, reliable and economic manner, built on advanced infrastructure and tuned to facilitate the integration of all involved. Smart grids possess demand response capacity to help balance electrical consumption with supply, as well as the potential to integrate new technologies to enable energy storage devices and the large-scale use of electric vehicles. [122]. 11, 12, 35

Software as a Service (SaaS) A service model where a cloud application is deployed at a provider's computing infrastructure (rather than at a users' desktop machines) and the developers of the application are able to roll smaller patches to the system and add new features without disturbing the users with requests to install major updates or service packs. Configuration and testing of the application in this model is arguably less complicated, since the deployment environment becomes restricted, i.e., the provider's data centre. Even with respect to the provider's margin of profit, this model supplies the software provider with a continuous flow of revenue, which might be even more profitable on the long run. [112]. 3, 4, 19, 37, 59, 74, 79

software-defined network (SDN) An emerging networking architecture that separates the control plane from the data plane in networking equipment. This is so that network intelligence and state are logically centralized, and the underlying network infrastructure is abstracted from applications. [83]. 12, 22, 80

SPI model (SPI) The three fundamental classifications of cloud service delivery are often referred to as the SPI Model, where SPI refers to Software as a Service (SaaS), PaaS, and Infrastructure as a Service (IaaS), respectively. [5]. 5, 80

Storage Area Network (SAN) A specialised network which consists of two tiers. The first tier, the storage plumbing tier, provides connectivity between nodes in a network and transports device-oriented commands and status. At least one storage node must be connected to this network. The second tier, the software tier, uses software to provide value-added services that operate over the first tier, such as to provide block-level network access to a consolidated data storage. [83]. 22, 80

Storage as a Service (StaaS) A service model that allows users to store their data at remote disks and access them anytime from any place. Cloud storage systems are expected to meet several rigorous requirements for maintaining users' data and information, including high availability, reliability, performance, replication and data consistency; but because of the conflicting nature of these requirements, no one system implements all of them together. [123]. 5, 22, 80

Supervisory Control and Data Acquisition (SCADA) A system used in manufacturing for acquiring measurements of process variables and machine states, and for performing regulatory or machine control across a process area or work cell. [83]. 12, 80

System for Cross-domain Identity Management (SCIM) An IETF standard created to simplify user management in the cloud by defining a schema for representing users and groups and a Representational State Transfer (REST) API for the necessary create, update, and delete operations. [124]. 56, 80

Transport Layer Security (TLS) A security protocol that provides privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. At the lowest level, layered on top of some reliable transport protocol, is the TLS Record Protocol, which provides connection security that has two basic properties: the connection is private and the connection is reliable. The TLS Record Protocol is used for encapsulation of various higher level protocols, such as the TLS Handshake Protocol, which allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. The protocol is a successor of SSL. [125]. 44, 63, 80

virtual factory (VF) An integrated simulation model of major subsystems in a factory that considers the factory as a whole and provides an advanced decision support capability. It allows mimicking the real life operations of the factory and it may server as a test bed for a real factory. [126]. 23, 59, 80

virtual private network (VPN) A system that delivers enterprise-focused communication services on a shared public network infrastructure and provides customized operating characteristics uniformly and universally across an enterprise. The term is used generically to refer to voice VPNs. To avoid confusion, Internet Protocol (IP)-based data services are referred to as data VPNs. Service providers define a VPN as a wide area network of permanent virtual circuits, generally using asynchronous transfer mode or frame relay to transport IP. Technology providers define a VPN as the use of encryption software or hardware to bring privacy to communications over a public or untrusted data network. [83]. 2, 22, 70, 80

virtual programmable logic controller (VPLC) A virtualised PLC that controls a particular manufacturing processes in the same way as a physical PLC. The virtualised PLC can be implemented, for example, as an integration of a software PLC into a real-time capable virtual machine. [23]. 12, 53, 80

virtual robot controller (VRC) A virtualised robot controller (RC) that monitors and controls robots in the same way as a physical RC. The virtualised RC can be implemented, for example, as an integration of a software RC into a real-time capable virtual machine. The VRC can be deployed as a cloud service, however, some of the features of RC must remain outside the cloud and near the controlled machine to preserve the real-time capability by using short communication paths. [23]. 12, 37, 80

WebSocket A protocol designed to work well with the existing Web infrastructure. A WebSocket connection starts its life as an HTTP connection, guaranteeing full backwards compatibility with the pre-WebSocket world. It allows to establish a full-duplex, bidirectional communications channel that operates through a single socket over the Web between a client's web-browser and a remote host. The protocol enables the two-way communication between the client running untrusted code in a controlled environment to the remote host that has opted-in to communications from that code. The security model used for this is the origin-based security model commonly used by web browsers. The goal of this technology is to provide a mechanism for browser-based applications that need fast and reliable two-way communication with servers. [127, 128]. 44

wide-area monitoring system (WAMS) A system to monitor assets over a large area, such as in the case of a power grid where operators continuously analyse all the features of a large power network in real time. The dynamic measurement system is using synchronized phasor measurement units with stability assessment and stabilization algorithms. It provides time-synchronized information on the measurement of phasors of voltage and currents in a power grid every 20 ms (in 50 Hz systems).

Each data sample is equipped with a time stamp and synchronized with a minimal accuracy. [129]. 35, 80

workforce performance management (WPM) A set of practices to automate and improve the processes and performance of employees in an organisation and therefore, to automate and improve the effectiveness of workforce processes. Its goal is to optimise performance levels and competency for the organization by better assignment of the employees to work processes in order to enhance productivity and profitability. The workforce management requires or is required by a recruit and hire management, compensation management, incentive management, goals management, learning management, competency management, performance measurement, and others. [130]. 21, 80

Acronyms

AEP Application Enablement Platform. 46

AI artificial intelligence. 45

AMQPS Advanced Message Queuing Protocol over TLS/SSL. 41, *see also Glossary:* Advanced Message Queuing Protocol over TLS/SSL (AMQPS)

API application programming interface. 5, 12, 14, 39, 41, 44, 65, 71, 74, *see also Glossary:* application programming interface (API)

AR augmented reality. 45–47, 49, *see also Glossary:* augmented reality (AR)

AWS Amazon Web Services. iii, 39, 40, 45, 46, 60

BAM business activity monitoring. 21, 23, *see also Glossary:* business activity monitoring (BAM)

BLOB binary large object. 55

BPM Business Process Management. 19–21, 23, 59, *see also Glossary:* Business Process Management (BPM)

BPMN Business Process Modelling Notation. 55, *see also Glossary:* Business Process Modelling Notation (BPMN)

CAD computer-aided design. 49

CC comparison criteria. 25, 37, 38, 40

CCM Cloud Cube Model. iii, 6, 7, 38, 39, 41–46, 50, 55, 56, *see also Glossary:* Cloud Cube Model (CCM)

CDN content distribution network. 21, 22, *see also Glossary:* content distribution network (CDN)

CMfg cloud manufacturing. 19, 20, 24–26, 28, 34, 35, 37–39, 41, 52, 53, 56–61, *see also Glossary:* cloud manufacturing (CMfg)

CNC computer numeric control. 12, *see also Glossary:* computer numeric control (CNC)

CPPS cyber-physical production system. 12, *see also Glossary:* cyber-physical production system (CPPS)

CPU central processing unit. 22, 30, 42

CRM customer relationship management. 19–21, 28, *see also Glossary:* customer relationship management (CRM)

CSA Cloud Security Alliance. iii, 32–34, 61

DaaS Data as a Service. iii, 14, 27, 28, 37, 38, 59, *see also Glossary:* Data as a Service (DaaS)

DAM/FAM database and file activity monitoring. 34, *see also Glossary:* database and file activity monitoring (DAM/FAM)

DAMA Design Anywhere, Manufacture Anywhere. 19, 20, *see also Glossary:* Design Anywhere, Manufacture Anywhere (DAMA)

DES discrete event simulation. 24, *see also Glossary:* discrete event simulation (DES)

DLP data loss prevention. 34, *see also Glossary:* data loss prevention (DLP)

DRM digital rights management. 34, *see also Glossary:* digital rights management (DRM)

ERP enterprise resource planning. 12, 19–21, 26, 27, *see also Glossary:* enterprise resource planning (ERP)

FTP File Transfer Protocol. 55, *see also Glossary:* File Transfer Protocol (FTP)

GE General Electric. iii, 40, 45, 54, 55, 57, 60, 61

GLBA Gramm-Leach-Bliley Act. 33

HIPAA Health Insurance Portability and Accountability Act. 33

HTTP Hypertext Transfer Protocol. 22, 41, 44, 55, 67, 75, *see also Glossary:* Hypertext Transfer Protocol (HTTP)

HTTPS Hypertext Transfer Protocol over Transport Layer Security. 44, 47, 51, *see also Glossary:* Hypertext Transfer Protocol over Transport Layer Security (HTTPS)

HW hardware. 1, 4, 5, 9, 21–23, 28, 30, 42, 43, 50, 51, 53, 56, 59

I/O input/output. 22, 30

IaaS Infrastructure as a Service. 3, 5, 9, 15, 19–23, 30, 32, 34, 37, 52–57, 59, 74, *see also Glossary:* Infrastructure as a Service (IaaS)

IdaaS Identity as a Service. 5, *see also Glossary:* Identity as a Service (IdaaS)

IoT Internet of Things. iii, 12, 15, 38–50, 54, 58–61, 70, *see also Glossary:* Internet of Things (IoT)

IP Internet Protocol. 7, 21, 30, 74, 75, *see also Glossary:* Internet Protocol (IP)

IT information technology. 1, 2, 7, 9, 15, 19, 27–31, 41, 48, 50–52, 55, 56, 59, 61, 63, 64, 68, 69, 73, *see also Glossary:* information technology (IT)

ITIL IT Infrastructure Library. 27, *see also Glossary:* IT Infrastructure Library (ITIL)

JSON JavaScript Object Notation. 56, *see also Glossary:* JavaScript Object Notation (JSON)

KPI key performance indicator. 14, 29, 38, *see also Glossary:* key performance indicator (KPI)

LDAP Lightweight Directory Access Protocol. 47, *see also Glossary:* Lightweight Directory Access Protocol (LDAP)

M2M machine-to-machine. 43, 45, 70

MaaS Manufacturing as a Service. 24, 37, *see also Glossary:* Manufacturing as a Service (MaaS)

MES manufacturing execution system. 12, *see also Glossary:* manufacturing execution system (MES)

ML machine learning. 45, 55

MQTT Message Queue Telemetry Transport. 39, 41, 42, 44, *see also Glossary:* Message Queue Telemetry Transport (MQTT)

MRP manufacturing resource/requirements planning. 19, *see also Glossary:* manufacturing resource/requirements planning (MRP)

NaaS Network as a Service. 5, *see also Glossary:* Network as a Service (NaaS)

NIST National Institute of Standards and Technology. 2–4, 6, 19

OPC-UA OPC Unified Architecture. 42, 50, *see also Glossary:* OPC Unified Architecture (OPC-UA)

PaaS Platform as a Service. 3–5, 9, 15, 19–23, 30, 32, 34, 37, 39–46, 49–51, 53–57, 59, 68, 74, *see also Glossary:* Platform as a Service (PaaS)

PCI Payment Card Industry. 33

PHM prognostics and health management. 23, 24, 59, *see also Glossary:* prognostics and health management (PHM)

PLC programmable logic controller. 12, 37, 50, 52, 54, 71, 75, *see also Glossary:* programmable logic controller (PLC)

QoS quality of service. 11, *see also Glossary:* quality of service (QoS)

RaaS Robot as a Service. iii, 12, 14, 37, 59, *see also Glossary:* Robot as a Service (RaaS)

RC robot controller. 12, 75, *see also Glossary:* robot controller (RC)

REST Representational State Transfer. 41, 44, 74, *see also Glossary:* Representational State Transfer (REST)

RFID Radio-frequency Identification. 12, *see also Glossary:* Radio-frequency Identification (RFID)

SaaS Software as a Service. 3–5, 9, 15, 19–23, 26, 27, 29, 30, 32, 34, 37, 40, 44, 45, 49, 50, 53, 54, 59, 74, *see also Glossary:* Software as a Service (SaaS)

SAML Security Assertion Markup Language. 44, 47, 56, *see also Glossary:* Security Assertion Markup Language (SAML)

SAN Storage Area Network. 22, *see also Glossary:* Storage Area Network (SAN)

SCADA Supervisory Control and Data Acquisition. 12, *see also Glossary:* Supervisory Control and Data Acquisition (SCADA)

SCIM System for Cross-domain Identity Management. 56, *see also Glossary:* System for Cross-domain Identity Management (SCIM)

SDK software development kit. 46

SDN software-defined network. 12, 22, *see also Glossary:* software-defined network (SDN)

SLA Service Level Agreement. 30, 53, 71, *see also Glossary:* Service Level Agreement (SLA)

SOA service-oriented architecture. 14, *see also Glossary:* service-oriented architecture (SOA)

SOX Sarbanes-Oxley Act. 33

SPI SPI model. 5, *see also Glossary:* SPI model (SPI)

SSL Secure Sockets Layer. 34, 56, 63, 74, *see also Glossary:* Secure Sockets Layer (SSL)

StaaS Storage as a Service. 5, 22, *see also Glossary:* Storage as a Service (StaaS)

SW software. 1, 4, 5, 9, 15, 16, 19, 21, 22, 24, 25, 27, 29, 30, 42, 43, 46, 48, 49, 54, 58–61

TLS Transport Layer Security. 44, 63, 67, 73, *see also Glossary:* Transport Layer Security (TLS)

UAA user account and authentication. 56

USA United States of America. 29

VF virtual factory. 23, 59, *see also Glossary:* virtual factory (VF)

VPLC virtual programmable logic controller. 12, 53, 57, *see also Glossary:* virtual programmable logic controller (VPLC)

VPN virtual private network. 2, 7, 22, 34, 70, *see also Glossary:* virtual private network (VPN)

VRC virtual robot controller. 12, 14, 37, 53, 57, *see also Glossary:* virtual robot controller (VRC)

WAMS wide-area monitoring system. 35, *see also Glossary:* wide-area monitoring system (WAMS)

WPM workforce performance management. 21, *see also Glossary:* workforce performance management (WPM)

XACML eXtensible Access Control Markup Language. 56, *see also Glossary:* eXtensible Access Control Markup Language (XACML)

XML Extensible Markup Language. 66, 73, *see also Glossary:* Extensible Markup Language (XML)