SN Computer Science (2023) 4:394
https://doi.org/10.1007/s42979-023-01815-z

ORIGINAL RESEARCH

Quality and Security Frameworks for IoT-Architecture Models Evaluation

Darine Ameyed[1] · Fehmi Jaafar[2] · Fabio Petrillo[2] · Mohamed Cheriet[1]

Received: 22 April 2022 / Accepted: 31 March 2023 / Published online: 15 May 2023

Abstract

The concept behind IoT is as powerful as it is complex, and for the entities and modules in the IoT solution to mesh together perfectly, they all must be part of a well-thought-out structure. That is where accomplishing a deep understanding, IoT architecture becomes paramount given the complexity of IoT domains and platforms. In this paper, we present a comparative analysis of IoT-architecture models based on IoT reference architecture proposed by ISO. Herewith, the paper aims at establishing a common grounding and language based on the business adoption reference IoT architecture vis-á-vis a standard model ISO/IEC 30141. We built an Analysis Architecture Quality Security Model-AAQSM based on quantitative metrics and scoring methods we have defined in reference to criteria standards. AAQSM helped unify evaluation metrics critical to fulfilling specific quality and security attribute requirements and classify architecture models by score.

Keywords Internet of Things · IoT architectures · ISO · Evaluation architecture approach · IoT security · Security standard · Quality requirements

Introduction

The Internet of Things (IoT) refers to the set of devices and systems that interconnect real-world sensors and actuators to cyberspace and the Internet. This includes many different systems, such as smart homes and buildings, wearable devices for health and fitness, connected cars any many more monitoring devices including wireless sensor networks that measure the world around us such as air quality, and more. The growth of the number and diversity of IoT devices that are collecting data are extremely fast. Many studies estimate that there will be more than 100 billion connected objects by 2025. McKinsey Global Institute predicts the IoT Market to be around 10 trillion US dollars by 2025 [1].

There are two key aspects to the development of IoT solutions: the devices themselves and the platforms-side architecture that supports them. Nevertheless, there are several challenges in developing IoT solutions: the lack of comparative frameworks that quantify the quality and security of these solutions, the diversification of the IoT architectures, and the variety of needs and usage of IoT solutions. Also, there remains a great deal of work to be carried out to develop appropriate evaluation approaches centered on the IoT system architecture models [2]. Pratap Singh [2] proposes three different classifications for the IoT architectures: (i) domain-specific architectures, (ii) layer-specific architectures, and (iii) industrial or commercial defined architectures. In the commercial context, we spotted a variety of IoT Reference Architecture (IoT-RA) models used and presented by the providers. Thus, it is necessary to make a comparative study of IoT-RA in accordance with a standard reference model to be able to deeply understand the commercial proposals and maps their similarities and differences.

Fehmi Jaafar, Fabio Petrillo, and Mohamed Cheriet have contributed equally to this work.

✉ Darine Ameyed
darine.ameyed.1@ens.etsmtl.ca

Fehmi Jaafar
fehmi.jaafar@uqac.ca

Fabio Petrillo
fabio@petrillo.com

Mohamed Cheriet
mohamed.cheriet@etsmtl.ca

[1] Systems Engineering Department, École de Technologie Supérieure (ÉTS), 1100 Rue Notre Dame O, Montreal, QC H3C1K3, Canada

[2] Department of Computer Sciences and Mathematics (DIM), at Quebec University at Chicoutimi (UQAC), 555 Bd de l'Université, Chicoutimi, QC G7H 2B1, Canada

The International Standardization Organization (ISO) specified a standardized IoT Reference Architecture using a common vocabulary and reusable designs. It covers four architecture views: functional view, system view, networking view, and usage view. The standard identifies the characteristics of IoT system into a generic IoT Conceptual Model. Studying the standard, exploring the architecture characteristics, and mapping the AR providers models, we identified the possibility to build an evaluation approach based on a set of reference standards. The proposed evaluation framework aims to help IoT systems' designers and developers meet all the principles and criteria which emphasis has been placed on for the IoT systems' requirements.

One of the main contributions of this paper is the presentation of a comparative analysis of four of the top commercial Reference Architecture (RA) Models as ranked in [3]. Our comparative analysis is based on the ISO/IEC 30141 reference IoT architecture [4]. Concretely, we are highlighting the similarities on domain-based ISO RM, with an exposure of the security capabilities of each provider. Last but not least, we provide in this paper a quantitative approach for IoT architecture evaluation based on specific frameworks for Analysis Architecture Quality Security Model (AAQSM).

The remaining paper is organized as follows: We start by providing an overview about the IoT-Architecture surveys and studies over the related work section. We present the ISO/IEC 30141 reference model explaining the outline of the standard with a specific focus on the domain-based model. Then, we provide a description of each commercial provider reference model followed by an analysis of similarities with the ISO standard. Thereafter, we introduce our evaluation approach including the quality and security frameworks driven by examples of evaluation of two commercial Reference Architectures. Then, we discuss the results and challenging point in IoT-architecture models. Finally, we conclude the paper with our main observations and future work.

Related Work

In the literature, multiple studies have analyzing IoT-architecture based in different categorizations such as layer-based architecture [5, 6], domain or sector-based models, also, commercial and industry defined models [3]. Those surveys aim to provide systemic classifications of different IoT architectures. Alshohoumi [7] performed a systematic review of existing IoT architectures including a set of 144 studies from 2008 to 2018. They provided a classification based on the number of layers and the features deployed in each layer. Pratap Singh [2] studied industrial IoT architectures and described the differences between them. Same classification studies were performed in [6]; adding specific domain-based models [3] have provided a survey identifying specific challenges depending in the application domain specifications. Ammar [8] presented a survey on security considerations in eight IoT architectures.

Even though those studies have performed systemic reviews on IoT architecture models, surveys of the IoT landscape and highlight technical challenges such as interoperability, scalability, security, energy efficiency, etc, still remain a remarkable gap on evaluation IoT-Architecture model studies and tools.

A recent paper has proposed an evaluation study [9]; they report multiple reference commercial models and provide evaluation analysis based on architecture criteria. However, they did not drive any similarities analysis, quality performance, or security focus. Which are of paramount importance as assessed and concluded in several studies [5, 10–13].

To facilitate future research and to help the solution designers and developers understanding the IoT system architecture models, this paper contributes investigation and analysis of providers' reference architecture models based on ISO standards which can help the developers' comparison of widely used commercial providers' architecture capabilities. We analyze the RM model following ISO/IEC 30141 standards using the ISO RM-domain-based model as a reference to highlight similarities with focus on security capacity. Furthermore, through our current study, we present a qualitative approach for quality and security evaluation of IoT Reference Architecture.

ISO IoT Reference Model and Reference Architecture

In this section, we introduce the IoT Reference Architecture (IoT RA) defined in ISO/IEC 30141 [4], which we consider as our standard reference model.

The IoT RA outlines what the general structured approach for an IoT system shall be by providing an architectural framework. It delivers direction to guide designing and developing an IoT system. It also aims to provide a better understanding of IoT systems to the stakeholders of those systems. In this paper, we summarize essential aspects, characteristics, and architectural views aligned with the architecture description defined in ISO/IEC 30141. That reference model presents the following description:

- A Generic characteristic of IoT systems outlining the characteristics expected from an IoT system;
- A Conceptual Model (CM) describing a key concept characterizing an IoT system;
- A Reference Model (RM) providing the overall structure of the elements of the architecture;

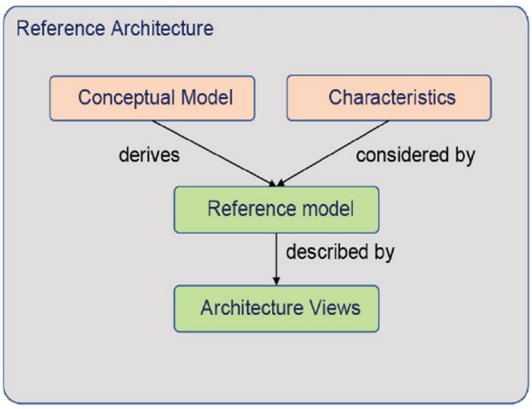

Fig. 1 IoT RA structure ISO IEEE 42010 [4]

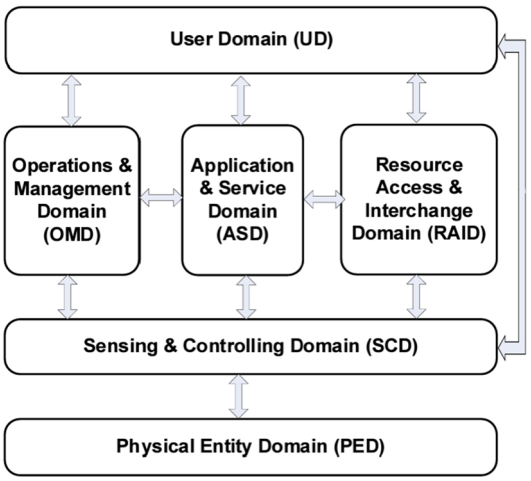

Fig. 2 Domain-IoT-based RM [4]

- Architecture views describing the architecture from several perspectives as functional views.

IoT RA Structure

The IoT RA is derived from a Conceptual Model (CM) and a set of characteristics defining a Reference Model including one or multiple architectural views, as it shown in Fig. 1. The characteristics include functional based such as context awareness, network, connectivity, etc., while others can be non-functional, such as integrity, availability, and compliance. In the other hand, the CM provides a common structure describing several vital concepts and the logical relations between the entities of an IoT System. Combined with the characteristics, it provides a background for Reference Model (RM) and the architectural views. ISO/IEC 30141 breaks down the CM into height system-level entity-based RM and domain-based RM. In this paper, we are mainly studying the Domain-Based Model.

Domain-Based IoT RM

The domains help the designers and developers of an IoT system to focus on various tasks that must be performed allowing a logical or physical subdivision. It is used to sort functions under different categories of responsibility, the main domains are: User Domain (UD), Operation and management Domain (OMD), application and services Domain (ASD), and Physical Entity Domain (PED), as shown in Fig. 2.

In our approach, we based our mapping providers' reference model with the ISO Domain-IoT-based RM. We summarize the ISO Domain-IoT based RM as follows:

User Domain (UD): Users are the actors of the UD. Users are both human and digital users. Human users interact with services via user devices, through which users access the IoT environment. Such devices can take many forms. Digital users interact directly with services through interfaces.

Operation and Management Domain (OMD): System operators and managers are the main actors of the OMD. They are responsible to maintain the overall good operation of the IoT systems. The OMD incorporates the primary functions responsible for provisioning, managing, monitoring, and optimizing the general systems' operational performance. The OMD typically includes the operation support system (OSS) and business support system (BSS), the systems by which the IoT system is managed, respectively, from an operational and a business viewpoint. The OMD is also responsible for overseeing the secure decommissioning of the IoT system when needed.

Application and Services Domain (ASD): Application and service providers represent the main actors of the ASD. It offers services to the IoT-User in the UD. The ASD contains the applications and services offered by the providers. The users in the UD interact with the applications and services to satisfy their requests. They interact also with the entities in the SCD to obtain data or drive actions in the PED. The applications and services can be delivered through cloud services and interact with peripheral entities via the RAID involving external organizations and peer systems. In the ASD, the applications and services interact with components in the OMD which are responsible for managing the operational aspects.

Resources and Interchange Domain (RID): The RAID runs mechanisms by which exterior entities can gate the capabilities of the IoT system. The main external entities are users interacting via their devices and peer systems. The abilities of the IoT system are accessible and controlled via one or more service interfaces. The RAID encloses the controlled endpoints offering the services. The fundamental capabilities proposed by the RAID are implemented by one

or more of the other domains, basically the ASD and the OMD.

Sensing and Controlling Domain (SCD): IoT devices, sensors, and actuators are the principal actors of the SCD. The SCD consists of the sensors monitoring different aspects of the PED and, also, of the actuators which can act on the PED. It is a vital part of an IoT system which bridges between the cyber environment and the real world. This domain encloses other entities, such as IoT gateways, local data stores, and local services.

Physical Entity Domain (PED): It contains the Physical Entities in an IoT system. Thus, the PED is a central environment inside which an IoT system offers monitoring, sensing, and controlling functions.

In our study, we present each RM provider based on their references, we analyze their architecture by describing each component, layer, or domain, and give examples and analyze the similarity with the ISO RM, mainly the ISO Based-Domain RM. We review the commercial models based on the ISO RM Based-Domain RM, as a domain model generally serves as a tool for human communication between people working in similar domains or across different domains.

IoT Security

ISO/IEC 30141 described how proprieties such as safety, security, privacy and Personally Identifiable Information (PII) protection, resilience and reliability apply to IoT systems in the context of the IoT Reference Architecture. In fact, in accordance with ISO/IEC 30141, an IoT system should use an Information Security Management System to identify risks to the IoT system. Then, this system identifies and implements sets of security controls that are applied to the IoT system to address those risks. In addition, an IoT system product Security Life Cycle Reference Model to standardize a set of activities called "IoT system Security Controls".

However, as IoT security is not detail led deeply in ISO/IEC 30141, there is another standard that extends the principles of IoT Security and provides guidance on the principles, the risks, and corresponding information security and privacy controls to mitigate those risks for the Internet of Things. This standard is the ISO/IEC DIS 27400 Cybersecurity—IoT security and privacy—Guidelines.[1] In fact, this new standard identifies a set of 'risk sources' and 'risk scenarios' relevant to IoT. Then, it proposes a rational basis for the selection of security and privacy controls to mitigate those risks. In this paper, we will propose a framework to evaluate the security of IoT architectures based on this standard.

[1] https://www.iso.org/standard/44373.html.

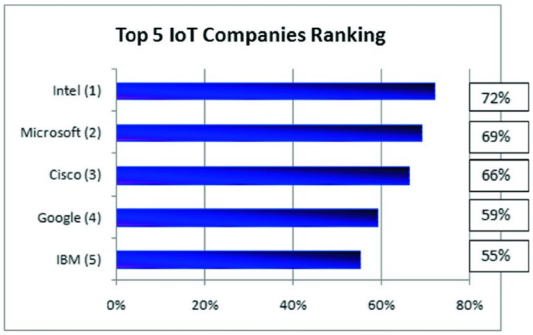

Fig. 3 Top IoT company [3]

Commercial RA Models and Mapping with ISO

The Internet of Things systems are paving the way towards success, providing solutions in different sectors. However, they still complexes to design, develop, and operate, and no single IoT architectural model can provide support for all domains and solutions. Lately, some providers have released their IoT platform reference architectures with the aim to standardize the complex and fragmented IoT industry, help giving an overview, and abstraction of their capabilities. However, a deep comprehensive analysis of the providers' reference models can provide a starting point for developers looking further for developing efficient and scalable IoT solutions. Using a standard like ISO can offer a highly valuable abstraction of the architecture model's main components and functionalities. Also, ease the valuation of the IoT-based system through different phases, design, implementation, operation, and maintenance. Further, provide a common approach to understand and compare providers' AR-Model capabilities, components, services, and functionalities. In this section, we perform an analysis and ISO-based mapping for RA-IoT models of the top-ranked providers, Fig. 3 [3]

.

Intel Reference Architecture

Intel Model Analysis

Intel proposed an IoT Reference Architecture [14] that contains three main components: things, network, and cloud. Intel presents their RM as a layer-based model including the following:

- Business and application layer, including components, e.g: APIs Libraries, Services orchestration, Business portal, API management portal, and product portfolio.

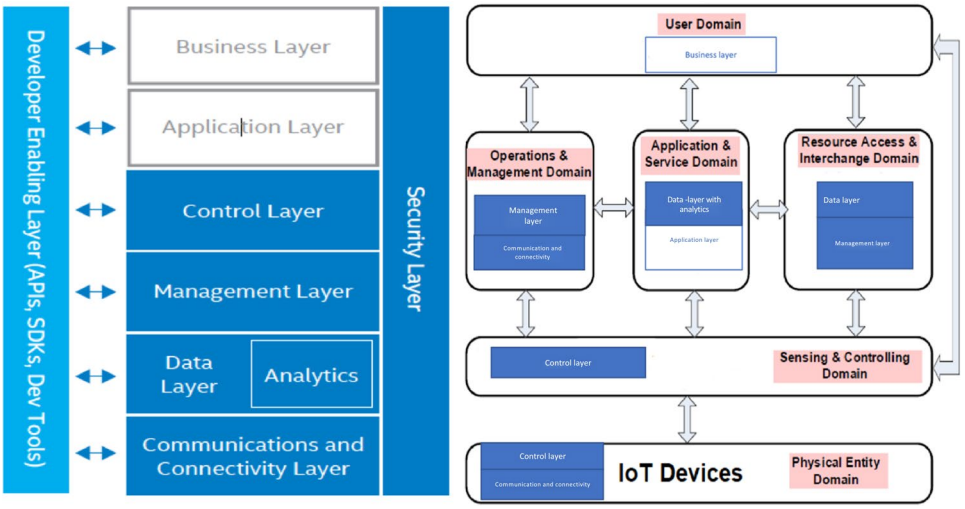

Fig. 4 Analysis of Intel IoT Architecture

- Communication and connectivity layers, including components, e.g.: Cloud data ingestion software, Enterprise services bus, Gateways, and Management agent.
- Data layer, including components, e.g.: Edge analytic agent, data agent, cloud data ingestion software, and operational DB.
- Management layer, including components, e.g.: Manage agent, devices cloud platform, data transport brokers, Management UI, Gateway, and Device agent.
- Control layer, including components, e.g.: Sensor hub, sensor handlers.
- Security layer, including components, e.g.: Intel HW security, McAfee embedded, ePolicy Orchestrator, and threat intelligence.

ISO vs. Intel

In this subsection, we analyze Intel RM through the ISO Domain-Based RM describing the similarities in function and services provided under each domain (Fig. 4).

User Domain (UD): As it can be easily observed, there is a considerable similarity between UD in ISO RM, the business and application layers on Intel RM. Those layers utilize the application layer as an access point to different services.

Operation and Management Domain (OMD): We observe a similarity with communication and connectivity layer, which support data ingestion and device control. Intel IoT RA performs broad protocol normalization, allowing multi-protocol data communication among devices at the edge as well as endpoint devices, gateways, the network, and the data center. It assures interaction with the edge data agent and ingests data coming from different devices. Also, we observe accordance with the data layer in which Intel IoT RA addresses the need of valuable insights generated by data analytics by distributing the analytics and control among the edge/cloud, gateways and end point devices. And so also, here is a similitude, with the management layer through which Intel IoT RA provides manageability function through the device cloud. Each managed device had an agent which connects the device to the cloud, updates software, and supervises devices. Device cloud function includes among others: discover, register and provision new devices, update application, manage data flows, upload or stream data, initiate action; manages access and users, etc.

Application and Services Domain (ASD): We noticed a similarity with business and application layer as they allow access point to many services. Also, there is a similarity in services provided by Intel RM in its data layer and analytics. The Intel service orchestration ensures service level agreements across resource managers. It can access operation databases and data, via ESB (Fig. 4).

Resources and Interchange Domain (RAID): Intel RA provides manageability functions through the device cloud via the management layer. It offers services to assure device management via device agents, data interchange via data transport brokers. Also, provide management for user interfaces and end users' access points.

Sensing and Controlling Domain (SCD) and Physical Entity Domain (PED): Those two domains present a similarity with the control layer in Intel RM. Intel provides directions to split up the management layer into a management plane and control plane with policy, control object, and APIs. Also, offer remote control via a cloud/centered control programming.

- **Security Capability**: Is a cross-domain capability trustworthiness. Security in Intel RA spans endpoint devices, the network, and the cloud providing end-to-end protection guided by MacAfee. It covers an endpoint device level, cloud level, and network level.

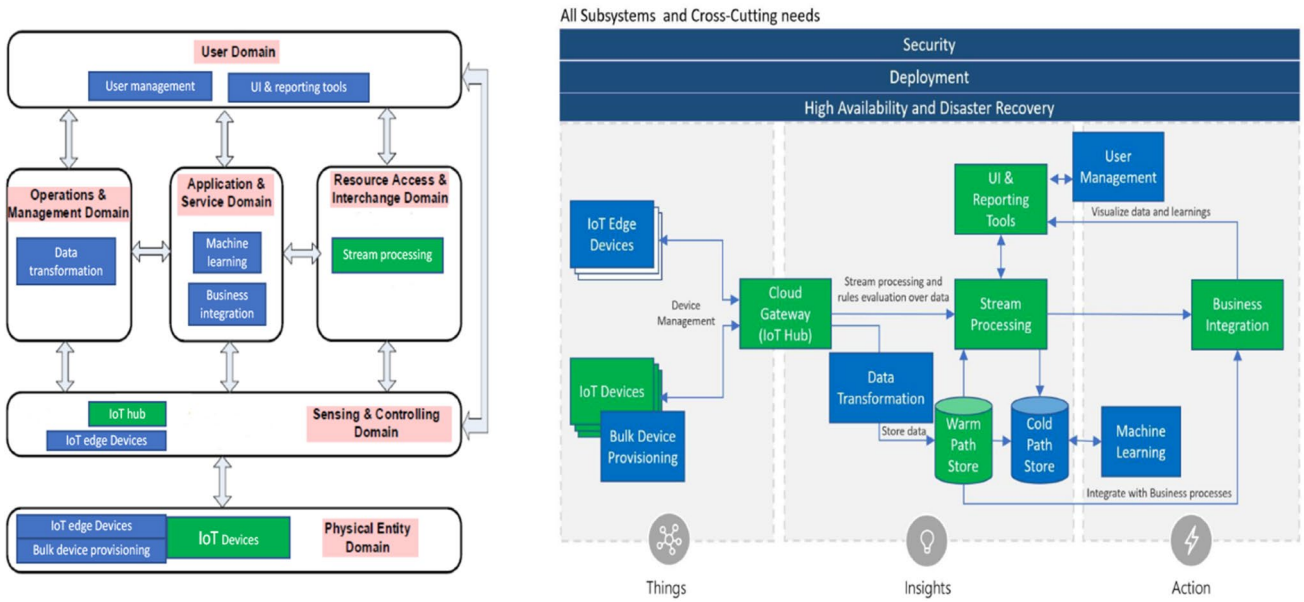

Fig. 5 Analysis Microsoft architecture

Microsoft Reference Architecture

Microsoft Model Analysis

Microsoft [15] present a reference architecture showing a recommended architecture for IoT application on Azure using platform-as-a-service (PaaS) component. This architecture consists of the following components:

- IoT devices, including components, e.g.: IoT devices, Edge IoT devices
- Cloud gateway, including components, e.g.: IoT hub.
- Device provisioning, including components, e.g.: IoT hub device provisioning services (DPS).
- Stream processing, including components, e.g.: Azure stream analytics, Azure databricks.
- Machine learning, including components, e.g.: Azure Machine learning.
- Warm path (WP) and Cold path (CP) storage, including components e.g.: Cosmos DB Azure and Blob storage.
- Data transformation, including components, e.g.: Protocol gateway, Azure function.
- Business process integration, including components, e.g.: Azure logic app.
- User management, including components, e.g.: Azure active directory.
- Security monitoring, including components, e.g.: Azure security center for IoT.

ISO vs. Microsoft

In this subsection, we analyze Microsoft RM through the ISO Domain-Based RM, Fig. 5.

User Domain (UD): We observed a similarity with the user management domain in the Azure model. It includes Azure activity directory and offers the possibilities of user management by restricting which users or groups can perform action on devices and, also, defines capabilities for users in applications.

Operation and Management Domain (OMD): We notice a similarity in functionalities related to data management in the intro/inter-domains level. Stream processing in Azure offers the possibility to join external data sources and manage the stream processing of data records. As well, we observe similarities with data transformation services in Azure as it provides different data management functionalities such as converting and combining data points before and after reaching IoT hub. Also, we notice data management capabilities on the Warm and Cold Path (WP) and (CP) as they provide the possibility of managing and holding data for short or long term. As well as in the user management domain Azure offers operation management in users' access and capabilities.

Application and Services Domain (ASD): We observe a similarity with Azure machine learning component which allows predictive algorithms to be executed enabling scenarios such as predictive maintenance. Also,

with Microsoft business process integration which performs action based on insights from the device's data, including sorting informational messages, and sending email and SMS. Those services are offered over the Azure logic app.

Resources and Interchange Domain (RAID): We notice a similarity with Azure stream processing over Azure data bricks and Azure stream analytic which offers complex analysis at scale using time windowing functions, also stream aggregations, and joins external data sources.

Sensing and Controlling Domain (SCD): Azure supports IoT devices on devices' level, edge, and cloud. Over the cloud gateway, Azure provides a cloud hub for devices to be able to connect securely to the cloud. Also, it provides device management and other capabilities, including command and control of devices. Via IoT hub, Azure offers a hosted cloud service that ingests events from devices, performing as a message broker between devices and back-end services. It also maintains a secure connectivity, bidirectional communication, and device management. IoT hub device provisioning services (DPS) help assign and register devices to specific Azure IoT Hub endpoints.

Physical Entity Domain (PED): Azure supports PED by offering the capabilities to IoT and edge devices to securely register and connect to the gateways and cloud.

- **Security Capability**: Azure offers Security monitoring via Azure security center for IoT which assures an end-to-end security solution for IoT workloads and simplifies their protection by providing a unified control and intelligent threat prevention, and detection, also responses across workloads from devices via Edge as well as up through the cloud.

Cisco Reference Architecture

Cisco Architecture Analysis

Cisco, Ref. [16] IoT Architecture is following a seven-layer model, as shown in Fig. 6. Each layer is specified in accordance with the ISO Reference Architecture to present an industrial architecture that may be globally accepted. For the data, on the one hand, it is considered in motion across the Physical Devices and Controllers level, the Connectivity level, the Edge/Fog level, and the Data Accumulation level. On the other hand, it is considered at Rest for the Data Abstraction level, the Application level, and the Collaboration Processes level. The Cisco IoT Architecture describes how tasks at each level should be handled and the relationships between levels.

ISO vs. Cisco

In this subsection, we analyze Cisco RM through the ISO Domain-Based RM reporting the similarities in function and services offered under each domain (Fig. 6).

User Domain (UD): We observed a similarity with the level 7 of Cisco IoT architecture, Collaboration and Processes. In fact, in this level, users interact directly with services through well-described interfaces. It includes Cisco Intersight, a software-as-a-service (SaaS) infrastructure lifecycle management platform that delivers simplified configuration, deployment, maintenance, and support for IoT platforms. In addition, we identify in this layer the Nexus dashboard, which can provide a unified operation view across diverse IoT platforms.

Operation Management Domain (OMD): We notice that no services or products are provided currently by Cisco for this domain.

Application and Services Domain (ASD): We notice a similarity with some functionalities in Level 6 is the application level that includes mobile applications, business intelligence reports, analytic applications, etc. For example, the Cisco Application Services Engine provides real-time analytics, visibility, and assurance for policy and infrastructure of IoT platforms.

Resources and Interchange Domain (RAID): We notice a similarity with some functionalities in Level 4, Data Accumulation, as the data in motion are converted to data at rest. This includes transforming the format of the data from network packets to database relational tables and achieving transition from "Event-based" to "Query-based" computing. In addition, the data abstraction in level 5 includes reconciling multiple data formats from different sources and confirming that data are complete to the higher-level application.

Sensing and Controlling Domain (SCD): Communications and connectivity are concentrated in Level 2 of the Cisco IoT architecture model. At the level 3 Edge (Fog) Computing, The Functions of Level 3 are driven by the need to convert data flows generated at the network level into data that can be used for storage and processing at the next Level (data accumulation).

Physical Entity Domain (PED): This domain is specified in Level 1 of the Cisco IoT architectures: Physical Devices and Controllers. However, we notice that no services nor products are provided currently by Cisco for this domain.

- **Security Capability**: Cisco specified an IoT Threat Defense framework that takes an architectural approach to protecting IoT. Among others, this framework attends to secure the devices and applications that are present on IoT platforms and to defend against high-risk activity on these platforms.

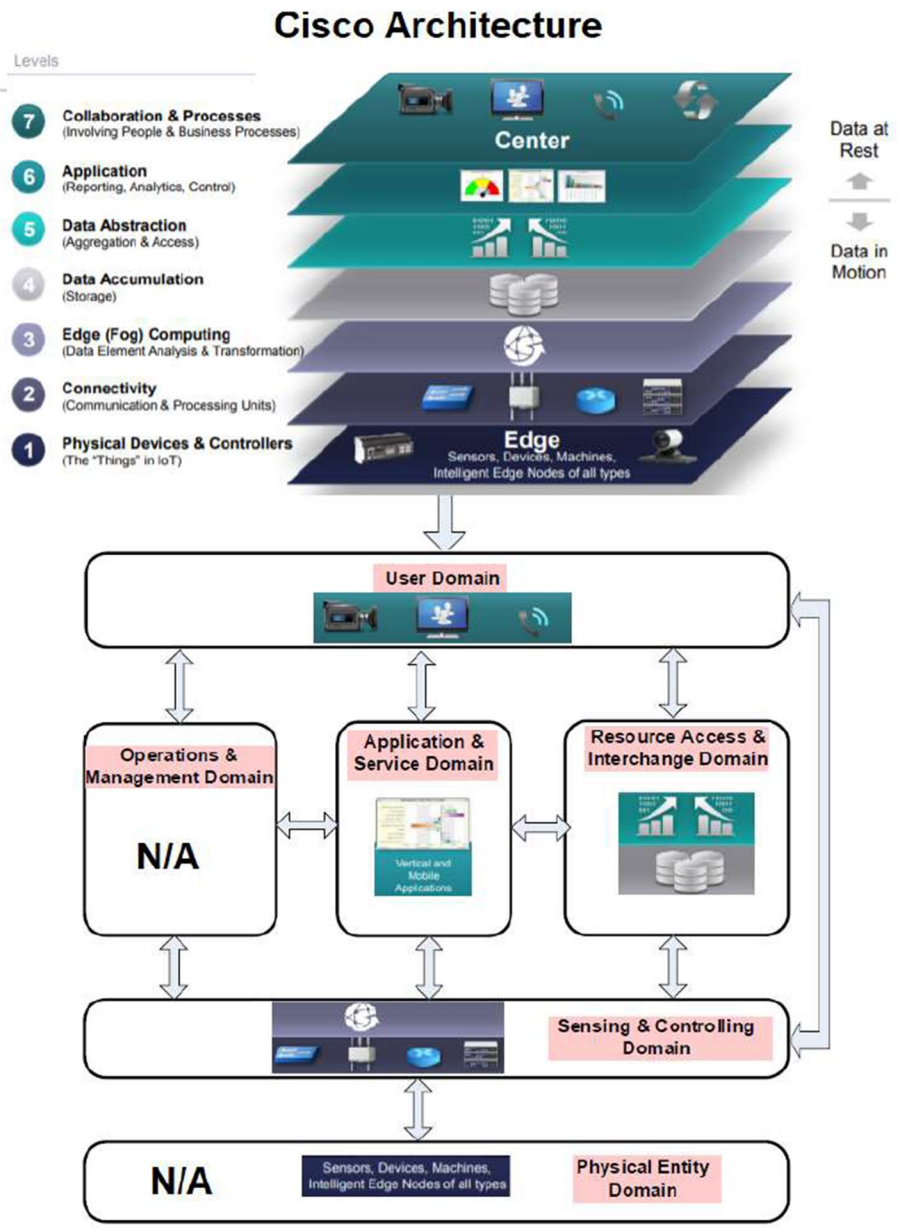

Fig. 6 Analysis of Cisco IoT Architecture

Google Reference Architecture

Google Architecture Analysis

Google Cloud Platform (GCP) presents an IoT architecture to connect IoT devices and manage/analyze their related data in the edge or the cloud [17]. In this architecture, we are observing that Google is following the ISO reference architecture with all its components, the device, gateway, cloud services and applications, and data usage systems.

The gateway can manage data on behalf of one or a set of devices. Its main role in the Google Reference Architecture is to ensure that devices can send the collected data to the cloud services even if they are not connected directly to the internet.

While identifying the similarities and divergence between Google architecture and ISO reference architecture, Fig. 7, we observed that there is a high emphasis in the Data Analytics in the Cloud. Indeed, the data from each device are sent to Google Cloud, where it is processed and combined with data from other devices to present the service layers (layer 3 in ISO), and potentially orchestrate the interaction with the human and digital users (layer 4).

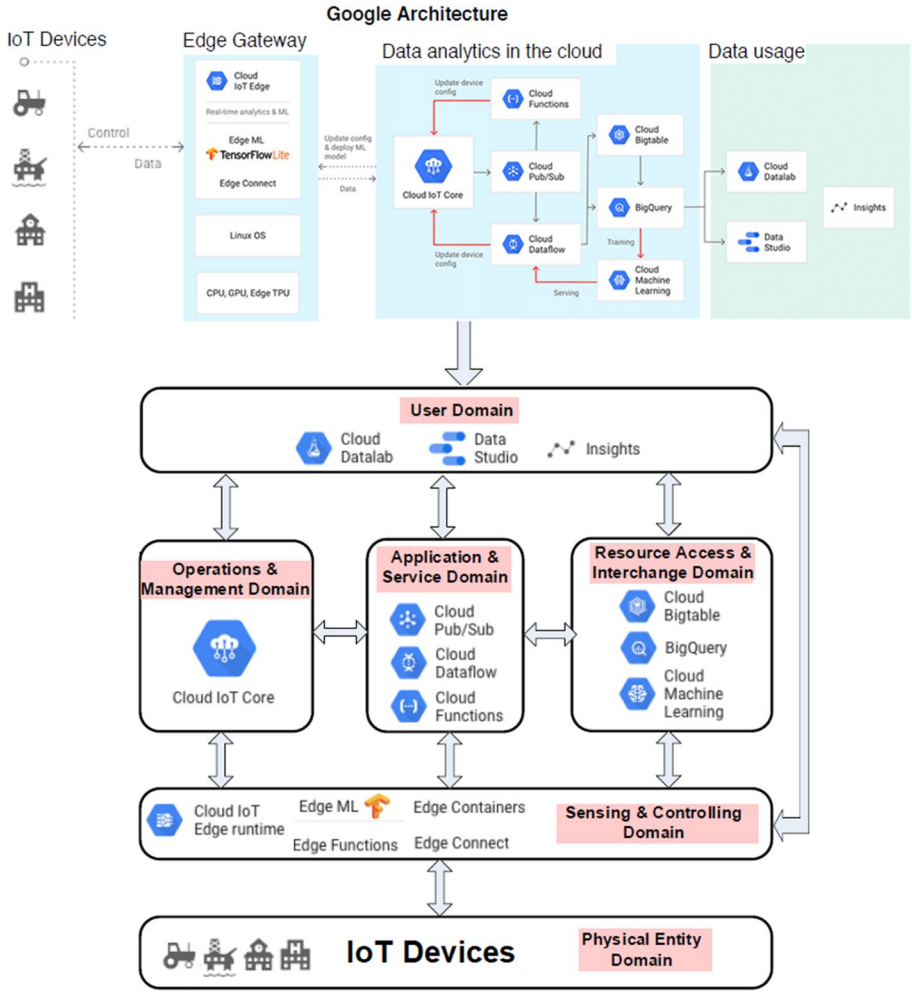

Fig. 7 Analysis of Google IoT Architecture

ISO vs. Google

In the following, we analyze Google RM through the ISO Domain-Based RM outlining the similarities under each domain, Fig. 7.

User Domain (UD)): Google IoT architecture ensures in this domain the interaction with data based on services, such as Datalab, Google Data Studio, and Google insights. Concretely, Datalab may be used by a user to interactively explore, transform, analyze, and visualize the data using a hosted online data workbench environment based on the open-source Jupyter project. In addition, the Google Data Studio is used to connect with IoT data and to visualize them through interactive reports. Finally, Google insights allows the detection of automated insights (that detects unusual changes or emerging trends in IoT data) and custom insights (that creates conditions that detect specific changes in IoT data).

Operation and Management domain (OMD): Google IoT architecture proposes IoT Core as a fully managed service for managing devices and secure their communications. This includes several tasks, such as the registration, authentication, and authorization if IoT devices inside the Google Cloud resource hierarchy, and the ability to send IoT device configuration from the service to IoT devices.

Application and Services Domain (ASD): According to Google IoT architecture, the application and services' domain are implemented through Cloud Functions which allows the users to write custom logic that can be applied to each event as it occurs. This is used to raise alerts, filter invalid data, or invoke other APIs. If the user needs to process data and events with more complex analytics, Dataflow provides analytic tools which can be useful to streaming and batch data including time windowing techniques and converging data from various streams. Finally, Pub/Sub offers a global and durable message ingestion service. The user can enable various components of an application to subscribe to specific streams of data without the need to construct subscriber-specific channels on each device, thus by creating topics for different streams or channels. Pub/Sub also allocates the users to connect to other Google Cloud services, such as ingestion, data pipelines, and storage systems, etc.

Resources and Interchange Domain (RAID): Google is presenting a set of AI and big data resources as mechanisms by which external entities can access the capabilities of the IoT system. For example, the Cloud Machine Learning provides fully configured environments to train models in the cloud with AI Platform Training services. On the one hand, BigQuery provides a fully managed data warehouse with a familiar SQL interface, so the user can store the devices data along with any of other enterprise analytics and logs. It also offers a better choice for queries that require data aggregation. On the other hand, Cloud Bigtable delivers a low-latency and high-throughput database for NoSQL data. It works better for queries that act on rows or groups of consecutive rows, as the Cloud Bigtable stores data using a row-based format.

Sensing and Controlling Domain (SCD): according to Google IoT architecture, this domain is presented as an Edge Gateway that manages and monitors the interchange of data with Cloud IoT Core. Several tools are ensuring this capability such as the Edge IoT Core runtime which connects edge devices to the cloud, allowing software and firmware to update and to manage data exchange with Cloud IoT Core. Moreover, Edge Connect is a Google component to connect IoT devices to the edge. In addition, users may use Linux OS services to connect IoT devices to the edge. As local services, we are identifying the Edge TPU, which can run AI at the edge. It brings high performance in a small physical and power footprint, allowing the deployment of high-accuracy AI at the edge. In addition, users may use GPUs or CPUs on Computing Engine instances to run your machine learning. We are also identifying the Edge ML runtime, which performs local ML inference using pre-trained models to reduce latency and increase the versatility of edge devices.

Physical Entity Domain (PED): For Google IoT architecture, this domain presents the IoT devices that detect physical signals and transform them to digital forms. The devices support voice commands and allow interaction with services through Google Assistant. Both in-house and third-party services are integrated, allowing various services for end users such as listening to music, controlling playback of videos or photos, or receiving news updates by voice. Some devices have integrated support for home automation, allowing users control smart home via voice command.

- **Security Capability**: In Google, IoT architecture is ensured through the secure services' deployment, secure data storage with end-user privacy protections, secure communications between services, secure and private communications between users and IoT devices. Concretely, the Cloud IoT Core offers a set of security features such as per-device public/private key authentication, Identity and Access Management (IAM) roles and permission, etc.

Proposed Evaluation Approach

Architecture evaluation is an important activity to assess the potential of a chosen model. It is a fundamental step in the development solution's roadmap in the aims to provide a system capable of fulfilling required quality requirements, also define potential risk. Due to the complexity of an IoT-architecture model, it has been very challenging to even have a reference architectural model as a consensus. In the past few years, as shown in the present paper, organizations, researchers, and practitioners have proposed RA models to ease the understanding of IoT architecture and the use of some existing solution frameworks. However, we still face a lack of evaluation tools to help developers and architectures to report an objective evaluation based on clear metrics and evaluation criteria. Thus, we propose an evaluation framework centered on architecture quality criteria based on ISO, also a security evaluation framework inspired by a compiling security reference and standards.

Evaluation Methodology

We propose an IoT reference architecture evaluation approach established on the Maximum Expectations (MAX-E) of an IoT-Architecture Model in functionality (Table 1), quality (Table 2), and security (Table 3). The Methodology is based on the following features:

- **Standard ISO/IEC 30141 IT-IoT RA**: Based on ISO 30141, the framework defines functional, architectural, and security criteria, described by the above-mentioned standards as the Main Characteristics of the IoT Systems.
- **Criteria score**: We specified scoring methods to define the existence or not, of a specific criterion. We are using as score 0 to 2, (0) Do not exist, (1) Partially exist or not clear, (2) Exist.
- **Relevance weight**: Derived from the level of relevance, as described by the ISO standard. We define a weight from 1 to 3: (1) Not relevant, (2) Relevant nice to have, and (3) Relevant must have.
- **Value criteria (V)**: Value is then a multiplication of the criteria score (S) by the criteria relevance weight:(W)
- **Total points value Architecture Model**: Is the sum of all the value criteria (defining j as the criteria index):
  $V(A) = \Sigma_j S.W.$

We tested our framework on two companies' models respecting confidentiality, ethic, and privacy, and we give the companies fictitious names, a company X and company Y instead of the commercial brand to assure the neutrality of our a scientific and research work.

Table 1 Functional criteria and architectural function evaluation

Functional criteria	R-Weight	MAX-E	Company X	Company Y
Accuracy	2	2	1	1
Auto-configuration	2	2	2	2
Compliance	2	4	2	2
Context-awareness	2	4	2	4
Content-awareness	2	4	2	2
Data (4V)	2	4	2	4
Discoverability	3	6	6	6
Self-description	3	6	6	3
Flexibility	1	6	6	3
Manageability	3	6	6	6
Network Management and Operation	1	2	2	2
Network Communication	3	6	6	3
Real-Time Capability	2	4	2	4
Service Subscription	2	4	2	2
	Score-Sum	60	47	44

Table 2 Architectural criteria and architectural quality evaluation

Architectural criteria	R-Weight	MAX-E	Company X	Company Y
Composability	3	6	6	6
Functional and management operation	3	6	6	6
Heterogeneity	3	6	6	6
Highly distributed systems	2	4	4	4
Legacy support	2	4	4	4
Modularity	2	4	4	4
Network Connectivity	3	6	6	3
Scalability	2	4	4	4
Sherability	2	4	2	4
Unique identification	3	6	6	6
Well defined component	3	6	6	3
	Score-Sum	56	54	50

Architecture Quality Evaluation Framework

Quality architectural evaluation reveals risks in the system design, and also brings central information about architecture components and functionalities. As the IoT solution is a pervasive system including different views, it can be approached by the entities-based or functional-based view as described in the preliminary sections ISO model and RA mapping.

Architecture Quality Evaluation Criteria

Architecture quality evaluation is based on architectural criteria and functional criteria as described in detail below.

Architectural Criteria

- **Functional and Management Capability Separation**: Functional interfaces and IoT component capabilities are properly separated, offering different endpoints for the management interface and functional interface which need to be handled by different software components.
- **Composability**: Is the ability to congregate various discrete IoT components into an IoT system to accomplish a set of objectives. Heterogeneity: Is the ability to support a various set of components, and logical and physical entities of an IoT system that interact in different ways.
- **Highly Distributed Systems**: It defines systems that, while being functionally integrated, include subsystems that can be physically separated in various and remote locations.
- **Legacy Support**: Is the concept that an IoT system might need to incorporate existing installed components, even where these components embody technologies that are no longer standard or approved. A service, protocol, device, system, component, technology, or

Table 3 Security criteria and security assurance evaluation

Security criteria		R-Weight	MAX-E	Company X	Company Y
Availability		3	12	6	3
First Sub Criteria	Secure Data Storage	3	6	6	3
Second Sub Criteria	Service Availability Assurance	3	6	0	0
Confidentiality		2	8	4	2
First Sub Criteria	Data Possession Management	2	4	0	0
Second Sub Criteria	Identity and Access Management	2	4	4	2
Integrity		3	12	6	3
First Sub Criteria	Vulnerability Assessment of IoT Devices	3	6	6	3
Second Sub Criteria	Data Integrity Assurance	3	6	0	0
Protection of Personally Identifiable information		2	8	2	4
First Sub Criteria	Privacy Assessment and Management	2	4	0	0
Second Sub Criteria	Privacy Protection	2	4	2	4
Reliability		1	4	2	4
First Sub Criteria	Failure Management	1	2	0	2
Second Sub Criteria	Security Threat Assessment	1	2	2	2
Resilience		1	4	0	4
First Sub Criteria	Fault Tolerance	1	2	0	2
Second Sub Criteria	Adaptability	1	2	0	2
Safety		1	4	0	4
First Sub Criteria	Implementation of Safety Standards	1	2	0	2
Second Sub Criteria	IoT Safety Protection	1	2	0	2
		Score-Sum	52	20	24

standard that is outdated but which is still in current use, can be incorporated into an IoT system.

- **Modularity**: Is a property allowing components to be combined forming larger systems, also easily removed and replaced with a similar size module or logical and physical interface.
- **Network Connectivity**: Communication capability is a core concept of IoT. It enables various other IoT characteristics including composability, resilience, share's ability, scalability, and discoverability.
- **Scalability**: Is the ability of a system to continue working effectively as the size, complexity, and volume of the system's workflow is increased.
- **Shareability**: It defined as the capacity of a system's component to be accessed and its resources allocated communally among different interconnected systems.
- **Unique Identification**: Is the characteristic of an IoT system to clearly and repeatedly associate the entities within the system using individual code, symbols, or numbers, which allow easy interaction with those entities and enable control and trace of their activities.
- **Well-Defined Components**: It allows an accurate description of the capabilities and characteristics of the system's IoT entities including associated uncertainties, configuration, security, etc.

Functional Criteria

- **Accuracy**: Depending on the context, an appropriate level of accuracy is necessary and might be required for the IoT system deployment and operation.
- **Auto-configuration**: It defines the devices automatic configuration based on their predefined interworking rules, which allow the IoT system to react to specific devices also conditions to their addition or removal. It is useful for large-scale IoT system to dynamically react to different changes.
- **Compliance**: Is the characteristic of conforming to different rules, regulation, standard, and policy. Deployment of IoT system can require adherence to a various of regulation and law which may need specific configurations to assess the IoT devices and system to function in certain context usage.
- **Context-Awareness**: Is the ability to monitor its own environment in which the device or the system is operating, based on real-world observation and information, such as time, location, and more. Context-awareness allows IoT systems to be flexible and user centric.
- **Content-Awareness**: Is the characteristic of having good enough knowledge of the information in an IoT

entity and its associated metadata which support appropriate functional operations.
- **Data Characteristics (4v)**: The data 4Vs derives from big data system characteristics, as the IoT systems are the source of large volume data, generated from diverse locations and with a wide variety of data types.
- **Discoverability**: Defines the ability of an endpoint on the network to be dynamically found and reports its services and capabilities through a query or a self-advertising mechanism.
- **Flexibility**: Is the ability of an IoT entity or system to provide a various range of functionalities suitable to a specific need or context.
- **Service Subscription**: As IoT system services are often established in the basis of the subscription model, it is important that the IoT service provider designs, operates, and maintains a clear mechanism for the subscriptions.

Security Assurance Evaluation Framework

It is commonly used to define the security as the combination of availability, confidentiality, and integrity. More specifically in ISO/IEC 20924, trustworthiness is defined as follows: "Degree of confidence that a stakeholder has that the system performs as expected with characteristics including safety, security, privacy, reliability and resilience, in the face of environmental disruptions, human errors, system faults and attacks." Inspired by this definition, by the ISO specification of IoT security described in ISO/IEC DIS 27400 Cybersecurity—IoT security and privacy—Guidelines,[2] we are proposing to evaluate the security of IoT architectures based on a set of criteria, we identify their relevance in accordance with the ISO Reference Architecture.

Security Criteria

Availability: This property means that the IoT architecture provides ways to ensure the continuous accessibility and usability of devices, data, and services by an authorized entity. We select the following two considerations in this propriety:

- **Secure Data Storage**: The user needs to store data generated from the Internet of Things and these data grow exponentially. We will evaluate whether the proposed architecture allows the user to store the IoT data on the cloud securely to be available in a timely manner.
- **Service Availability Assurance**: We will evaluate whether the proposed architecture can provide the required availability in a resource-efficient manner, by dynamically providing failure detection in IoT services and recovery function according to service characteristics.

Confidentiality: This property means that the IoT architecture provides ways to protect sensitive data to being available or disclosed to unauthorized entities. We select the following two considerations in this propriety:

- **Data Possession Management**: We will evaluate whether the proposed architecture record data origins, and manage the data possession and the history of data generation with processing.
- **Identity and Access Management**: We will evaluate whether the proposed architecture provides a way for management Identity Access Management by identifying users and things (this includes user authentication, authorization, and consent).

Integrity: This property means that the IoT architecture provides ways to protect sensitive data to being available or disclosed to unauthorized entities. We select the following two considerations in this propriety:

- **Vulnerability Assessment of IoT Devices**: We will evaluate whether the proposed architecture includes a process of identifying, quantifying, and prioritizing the vulnerabilities in IoT devices.
- **Data Integrity Assurance**: We will evaluate whether the proposed architecture ensures that data collected, shared, and stored in IoT is complete, original, consistent, attributable, and accurate.

Protection of Personally Identifiable information: This propriety includes several principles to be handled by the IoT architecture, such as consent management, information collection limitation, and data minimization.

- **Privacy Assessment and Management**: We will evaluate whether the proposed architecture provides a way to assess privacy risks associated with IoT systems.
- **Privacy Protection**: We will evaluate whether the proposed architecture provides sensitive Data Protection through mechanisms such as anonymization.

Reliability: This property means that the IoT architecture provides ways to ensure that the data are consistent, and the communication is following an intended behaviour. We select the following two considerations in this propriety:

[2] https://www.iso.org/standard/44373.html.

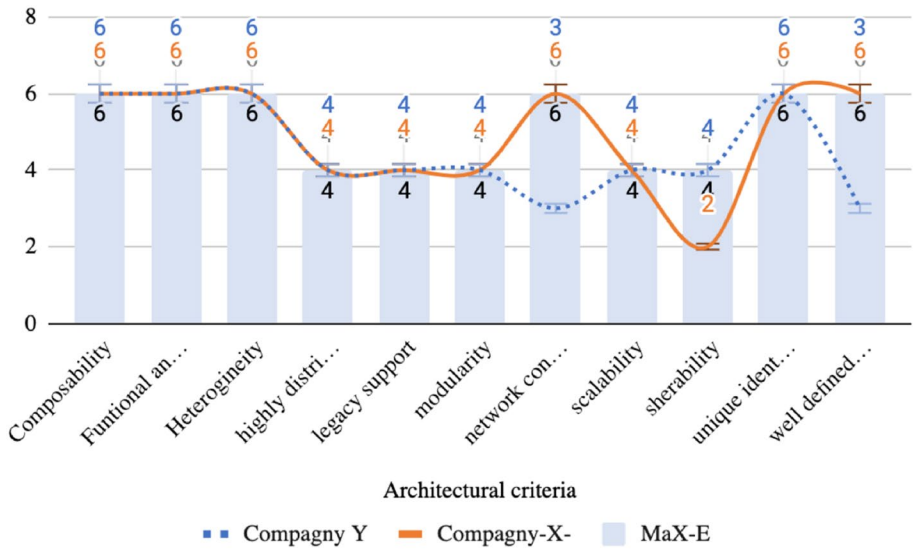

Fig. 8 Architectural Evaluation

- **Failure Management**: Failures in IoT can be due to hardware, software, connectivity, or unexpected adverse conditions. We will evaluate whether the proposed architecture provides the ability to log and retry failures in IoT platforms.
- **Security Threat Assessment**: We will evaluate whether the proposed architecture assesses threats and risks which consider the dynamics and uniqueness of IoT.

Resilience: This property means that the IoT architecture can adapt its component to continue to implement its functions regardless changes and faults. We select the following two considerations in this propriety:

- **Fault Tolerance**: We will evaluate whether the proposed architecture ensures a fault-tolerant IoT.
- **Adaptability**: We will evaluate whether the proposed architecture can adapt and evolve to defend against future threats.

Safety: This property means that the IoT architecture is making proper consideration of safety factors. We select the following two considerations in this propriety:

- **Implementation of Safety Standards**: This includes compliance with safety standards.
- **IoT Safety Protection**: We will evaluate whether the proposed architecture provides mechanisms of preventing, reducing, or mitigating the potential for undesired outcomes; specifically, damage, harm, or loss.

Results and Discussion

Generic Result

Tables 1, 2 and 3 presents our evaluation approach based, respectively, on functional, architectural criteria and security assurance requirements. We describe criteria, weight, and scoring for each category. We provide a reference score Max-E and we generate scoring for two IoT-Architecture models, developed by two worldwide companies, we called "Company-X" and "Company-Y".

The Score-Sum provides a global score for each category compared to the MAX-E reference score. The presented graphical evaluation of the Company X and Y vs. the scores of MAX-E, for the purpose to have a reference to best architectures scores values (Figs. 8, 9 and 11).

Regarding the architectural quality, Fig. 8, we observe that the companies reach the average or the max of each criterion and attain a high sum score near the sum MAX-E. That is due to the fact since the provider tries to cover different needed components supporting IoT solutions. Still, the network communication is not a component provided or supported clearly by different providers.

A rather similar trend can be observed among functional criteria Fig. 9 but with an exception on specific criteria regarding more cognitive capacities and data management, such as context awareness, content awareness, data, etc., which likely indicates a business focus of certain providers' services on offer (see Fig. 10).

A global scores are presented in Figs. 11, 12, and 13.

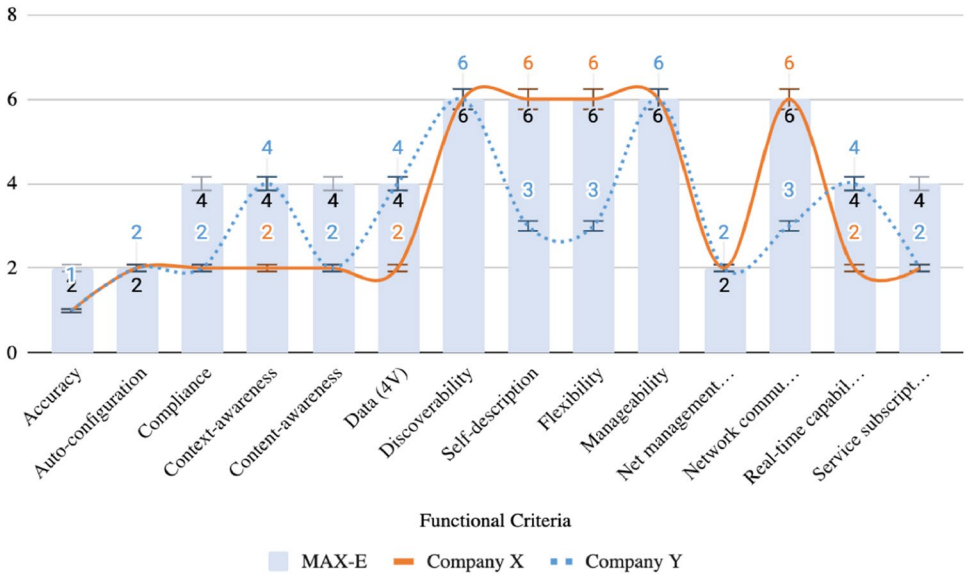

Fig. 9 Functional evaluation

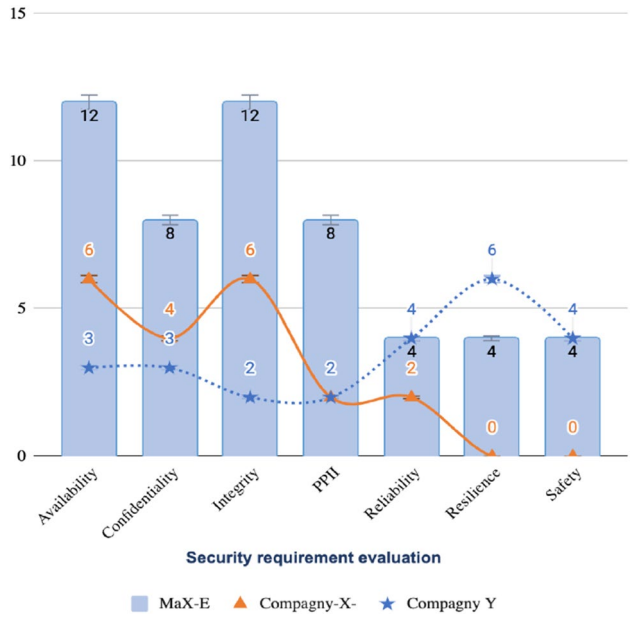

Fig. 10 Security assurance evaluation

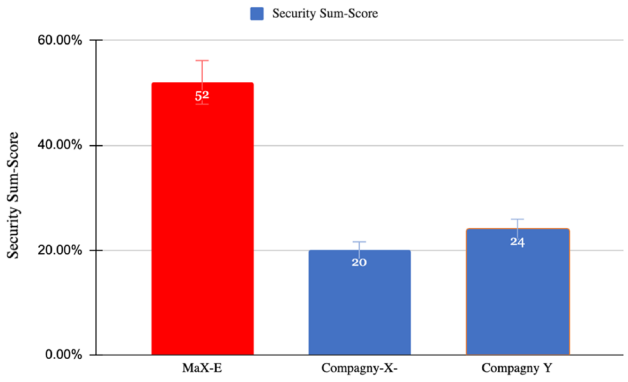

Fig. 11 Security score

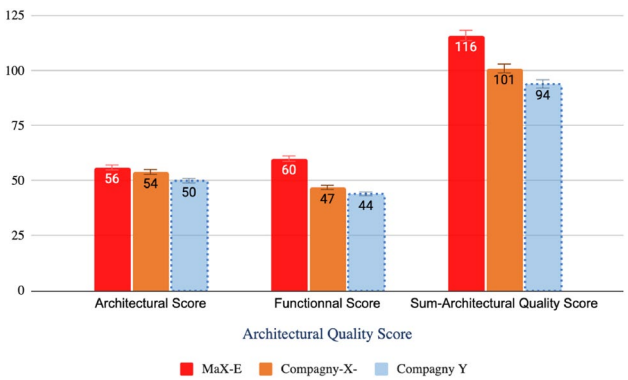

Fig. 12 Architectural quality total score

Discussion

Following the need of offering a deep understanding of the existing Reference IoT architecture and the urgent necessity of a common vocabulary, we have investigated the state-of-the-art of the top existing IoT Reference model presented by the commercial provider. Which we analyzed and mapped based on ISO reference architecture.

By choosing a referential standard model as ISO, we could evaluate different architectures in accordance with an international standard that defines the functionalities and capabilities that an IoT architecture must provide. As expected, we observe that there is no single consensus on IoT architecture. The complexity of the IoT domain, as well as the diversity of IoT-based solutions, are among others, reasons for differences among the IoT architectures. The

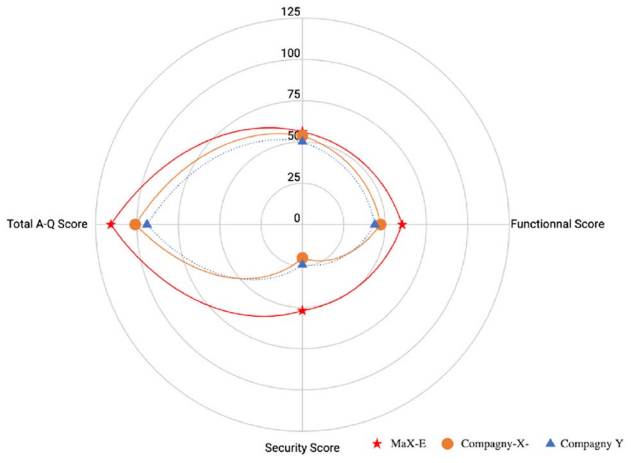

Fig. 13 Total evaluation score

proposed study and mapping approach aim to provide a common tool for architecture analysis that may be used by developers and designers across different domains, including different stakeholders and end users.

ISO RM proposes a structured architecture combining views and characteristics which we used to classify the functionalities of the different providers' RM components. There is no obligation for any IoT system for those characteristics defined by the ISO entities-based or domain-based reference model. However, it is still essential for any IoT architect to reflect those concepts in his design. In another hand, the ISO model offers a common structure describing fundamental concepts and the logical relations between the entities of an IoT System. Combined with the characteristics it provides, a background for the Reference Model (RM) and the architectural views which were the basis of our analysis approach and the fundamental vital component for a robust IoT-based solution.

Given the importance of the security aspect, we had a specific analysis point on the security capability. As noted, the providers present their model including security capabilities; however, not all of them provide specific security capabilities for each domain. We also noticed the absence of any specific protocols discussing privacy along the data life cycle; which is also unfortunately absent on ISO reference document under any clear and precise recommendations to tackle security and privacy issues or/and policies.

Inspired by the ISO RM and quality criteria combined with security assurance concepts and standard, we specified an evaluation framework for IoT-architecture models.

To provide a clear and granular approach, we defined architectural quality evaluation centered on multiple criteria and sub-criteria where needed. We specified an architectural quality framework evaluation based on architectural and functional criteria. We have observed a global trend in respecting the main and mandatory requirement for functionality as flexibility, scalability, manageability, auto-configuration, and self-description. Also, for the specific IoT system expectations such as discoverability, legacy support, modularity, unique identification, well-defined components and highly distributed system capacity, Figs. 8 and 12. However, some criteria remain not clear in the provider reference architectural RM description or not covered. This may be due mostly to the business focus and market trend which still way from adoption of some integration related to the data valorization and cognitive capacities on the IoT systems. Particular attention must be paid to improving the awareness capacities of the systems as context [18, 19] and content awareness and also data management and analytic services [20, 21].

In Table 3 and Fig. 10, we showed a ruining example of our proposed security framework by evaluating two of the most used IoT architectures. Our evaluation showed a clear lack of security criteria implemented in IoT architectures. Indeed, in the absence of a mandatory standard for basic security implementation, IoT manufacturers only focus on device functionality [22]. For example, we noticed that the analyzed IoT architectures do not present mechanisms to check for vulnerabilities in the IoT platforms, or in the associated applications.

The most common reason behind this fact is that the first and sometimes the only priority of IoT providers is to reduce production costs and speed time to market [23]. Concretely, many IoT manufacturers prioritize convenience over security [24]. Although some IoT architectures provide privacy and security protections, this protection is still far from the required one described in ISO standard.

As an increasing number of IoT-connected devices make massive entry into our ecosystem, companies need to carefully assess the security capabilities of the IoT providers and their related architectures. Currently, the security personnel are already busy with frequent, but relatively minor vulnerabilities, they will find it difficult to cope with new potential and damaging risks related to IoT platforms [25].

Conclusion

With the diversification of IoT tools and solutions, it became hard to evaluate and to compare the different IoT architectures. Thus, we presented a study that compares a set of the most adopted IoT architectures in accordance with the ISO reference model. In addition, inspired by the quality and security criteria specified in that standard, we presented an evaluation framework, AAQSM, that evaluates the quality and the security of IoT architectures. We aim that our study benefits researchers that performing comparative analysis of IoT architectures and enthusiast that needs to choose

the most suitable IoT providers in accordance with ISO recommendations.

More models' data can provide a deeper analysis of the quality and security of IoT architecture. It will also allow a richer metric to estimate deviation calculated based on impact which we were not able to have any information about it. Once available, a dynamic assessment quality and security framework can be developed it.

Our future work includes (i) a quantitative analysis and a systematic literature review of IoT architectures, including industrial and open-source platforms (ii), and the exploration of correctness measures to improve the quality and the security of IoT architectures.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Ahmed BS, Bures M, Frajtak K, Cerny T. Aspects of quality in internet of things (iot) solutions: A systematic mapping study. IEEE Access. 2019;7:13758–80. https://doi.org/10.1109/ACCESS.2019.2893493.
2. Pratap Singh S, Kumar V, Kumar Singh A, Singh S. A survey on internet of things (iot): layer specific vs. domain specific architecture. In: Smys S, Senjyu T, Lafata P. editors. Second International Conference on Computer Networks and Communication Technologies. Cham: Springer; 2020, p. 333–41.
3. Kaur H, Kumar R. A survey on Internet of Things (iot): layer-specific, domain-specific and industry-defined architectures. In: Advances in Computational Intelligence and Communication Technology: Proceedings of CICT 2019. Springer Singapore, 2021, p. 265–275.
4. ISO, IEC. Internet of things (Iot)—reference architecture. International Standard. 2018;2018:1–88.
5. Lin J, Yu W, Zhang N, Yang X, Zhang H, Zhao W. A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things J. 2017;4(5):1125–42.
6. Chanal PM, Kakkasageri MS. Security and privacy in iot: a survey. Wirel Pers Commun. 2020;115(2):1667–93.
7. Alshohoumi F, Sarrab M, Al-Hamdani A, Al-Abri D. Systematic review of existing iot architectures security and privacy issues and concerns. Int J Adv Comput Sci Appl. 2019;15:10. https://doi.org/10.14569/IJACSA.2019.0100733.
8. Ammar M, Russello G, Crispo B. Internet of things: a survey on the security of iot frameworks. J Inform Secur Appl. 2018;38:8–27. https://doi.org/10.1016/j.jisa.2017.11.002.
9. Boyanov L, Kisimov V, Christov Y. Evaluating iot reference architecture. In: 2020 International Conference automatics and informatics (ICAI), 2020; pp. 1–5. https://doi.org/10.1109/ICAI50593.2020.9311357.
10. Hassan WH, et al. Current research on internet of things (iot) security: a survey. Comput Netw. 2019;148:283–94.
11. Alaba FA, Othman M, Hashem IAT, Alotaibi F. Internet of things security: a survey. J Netw Comput Appl. 2017;88:10–28.
12. Zhao K, Ge L. A survey on the internet of things security. In: 2013 Ninth International Conference on Computational Intelligence and Security, 2013; pp. 663–667. IEEE.
13. Patnaik R, Padhy N, Srujan Raju K. A systematic survey on IoT security issues, vulnerability and open challenges. In: Intelligent System Design: Proceedings of intelligent system design: INDIA 2019. Springer Singapore, 2021. p. 723–730.
14. Intel. The Intel IoT Platform. https://www.intel.com/content/www/us/en/internet-of-things/white-papers/iot-platform-reference-architecture-paper.html. 2015. Accessed 17 Dec 2019.
15. Microsoft. Azure iot reference architecture. 2020. https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/iot. Accessed 11 Sept 2020
16. Cisco. The Internet of Things Reference Model. 2014. http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf. Accessed 6 Jan 2020.
17. Google. Technical overview of internet of things. 2020. https://cloud.google.com/architecture/iot-overview. Accessed 5 May 2021.
18. Ameyed D, Miraoui M, Zaguia A, Jaafar F, Tadj C. Using probabilistic temporal logic pctl and model checking for context prediction. Comput Inform. 2018;37(6):1411–42.
19. Mitra K, Ranjan R, Åhlund C. Context-aware Iot-enabled cyber-physical systems: a vision and future directions. In: Handbook of integration of cloud computing, cyber physical systems and Internet of Things. Springer; 2020, p. 1–16.
20. Flores M, Maklin D, Golob M, Al-Ashaab A, Tucci C. Awareness towards industry 4.0: key enablers and applications for internet of things and big data. In: Working Conference on Virtual Enterprises, 2018; p. 377–86. Springer.
21. Meurer RS, Fröhlich AA, Hübner JF. Ambient intelligence for the internet of things through context-awareness. In: 2018 International Symposium on Rapid System Prototyping (RSP), 2018; p. 83–89. IEEE.
22. Singh RP, Cassell B, Keshav S, Brecht T. Tussleos: managing privacy versus functionality trade-offs on iot devices. ACM SIGCOMM Comput Commun Rev. 2018;46(3):1–8.
23. Wei Z, Masouros C, Liu F, Chatzinotas S, Ottersten B. Energy-and cost-efficient physical layer security in the era of iot: the role of interference. IEEE Commun Mag. 2020;58(4):81–7.
24. Pearson B, Luo L, Zhang Y, Dey R, Ling Z. On misconception of hardware and cost in IoT security and privacy. ICC 2019–2019 IEEE International Conference on Communications (ICC). IEEE; 2019. p. 1–7.
25. Alam S, Siddiqui ST, Ahmad A, Ahmad R, Shuaib M. Internet of Things (IoT) enabling technologies, requirements, and security challenges. In: advances in data and information sciences: proceedings of ICDIS 2019. Springer Singapore, 2020, p. 119–126.