ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Survey on the State of development of the Standardized IoT Architecture

Pratiksha R.Shetgaonkar

Asst. Professor,Department of Computer Engineering, S.R.I.E.I.T, Shiroda, Goa, India

ABSTRACT*:* There has been ,is and will be much hype about the “Internet of Things”. The idea of a globally interconnected continuum of devices, objects and things in general emerged with the RFID technology, and this concept has considerably been extended to the current vision that envisages a plethora of heterogeneous objects interacting with the physical environment.

One key thing to understand is that, the IoT requires number of technologies to work from wireless communications, to data security, to intercommunications with so many other devices and so it’s very much unlikely that the single standard will cover all this.

Till now, there is no standardized architecture approved by an authorized body for IoT and many groups and organizations are working towards bringing a centralized & standardized architecture and standards in the world of IoT. As a result of this, different architectures for IoT are offered by various stakeholders.

In this paper, an attempt is made to study the different suggested IoT architectures offered by various projects, academic and industrial bodies. For the purposes of this paper, we have focused on the architectural model offered by some important & noteworthy groups and alliances as mentioned below.

- IEEE P2413 Architecture
- IoT-A Architecture
- The OIC Cloud Native Architectur
- The Cisco IoT/M2M architecture
- IDCArchitecture
- WSO2 Architecture
- Computing Community Consortium Architecture

KEYWORDS: Internet of Things; architecture; standards; IEEE P241; Cisco; IoT-A;OIC; IDC; WSO2; CCS

I. INTRODUCTION

Potential migration towards an Industrial Internet of Things (IIoT) raises numerous questions regarding suitable architectural frameworks or reference architectures for use in these emerging ecosystems. Organizations such as the IEEE (Institute of Electrical and Electronics Engineers), the Industrial Internet Consortium (IIC), and the European IoT-A (Internet of Things – Architecture) project, among others, look to provide architectural frameworks that define relationships between IoT domains and devices, as well as appropriate security schemes

Almost all of these IoT platforms provide a comprehensive set of generic, i.e. application-independent, functionalities that can be leveraged to build IoT applications.

The overall nature of IoT applications can be quite diverse. On the one hand, the architectures can be centralized system architectures in case of machine-to-machine applications such as fleet management and asset tracking which are often enterprise solutions that rely on, i.e. they build on one key enterprise application.

On the other hand, some architectures can be consumer-focused and decentralized without any central coordination authority such as those in the Smart Home domain .

While the two types of application ie centralized as well as decentralized still vary, for example in terms of their underlying technologies, there is a strong convergence of both domains.

DOI: 10.15680/IJIRCCE.2016. 0402022

II. Related work

Though many organizations work on the standardization process, [1] focused on those that work on IoT and provide a definition for it. Accordingly, [1] considered IoT definitions from ETSI, ITU, IEEE, the IETF, the NIST, the OASIS and the W3C.

In [2] the authors focussed on the Event Driven Architecture of IOT. In [4] the author discusses about some of the major standards being developed across ,as of mid-2015 and what the prognosis is for each of them. In [5] the author discusses about the IDC IOT architecture & believes that the IoT platform will be driven by the desire to be a leader in IoT device and data management, the challenge to connect IT companies with industry-based IT operational technology & the ability to remain relevant as more new companies with open architectures move quickly into this market.

In [10] the focus and scope of the paper is solely on the security aspects of the Internet of Things. In [8] the authors discuss about how the existing best practices in building robust and secure systems are insufficient address the new challenges that IoT systems and provide recommendations regarding investments in research areas that will help address inadequacies in existing systems, practices, tools, and policies.

The goal of this white paper[8] is to consider the core software, systems, and networking technology shifts created by the IoT trend and try to anticipate the major challenges such systems face in terms of usability, performance, security, and reliability.

The remaining papers[9],[11],[12] describes & discusses the IOT architecture proposed by the various groups & alliances

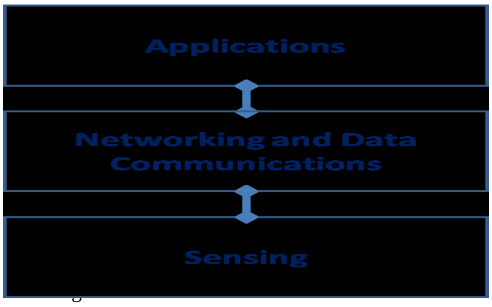
III. IOT ARCHITECTURES

A. *IEEE P2413 Architecture*

The scope of IEEE P2413 is to define an architectural framework, addressing descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities.

IEEE P2413 is currently considering the architecture of IoT as three tiered which is considered to be a Market Driven Architecture.

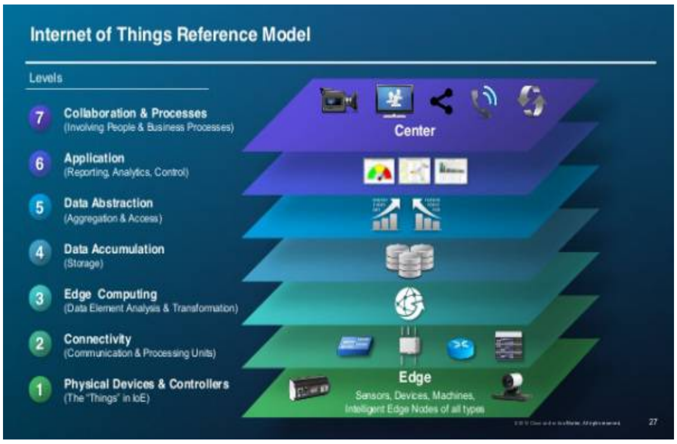
This architecture is a very generic in nature.



The all minute details of the architecture is available in IEEE white paper as mentioned in reference [1].

B. *IoT-A Architecture*

IoT-A, is the European Lighthouse Integrated Project, has addressed for three years the Internet-of-Things Architecture, and created the proposed architectural reference model together with the definition of an initial set of key building blocks. Together they are envisioned as foundations for fostering the emerging Internet of Things.



Internet of Things Reference Model

Levels

7 Collaboration & Processes (Involving People & Business Processes)

6 Application (Reporting, Analytics, Control)

5 Data Abstraction (Aggregation & Access)

4 Data Accumulation (Storage)

3 Edge Computing (Data Element Analysis & Transformation)

2 Connectivity (Communication & Processing Units)

1 Physical Devices & Controllers (The "Things" in IoE)

Center

Edge

Sensors, Devices, Machines, Intelligent Edge Nodes of all types

Fig2: IoT-A Reference Model

IoT-A Reference Model consists of 7 layers as described below:

1. **Physical Devices and Controllers**

The physical devices and controllers that might control multiple devices. These are the "things" in the IoT, and they include a wide range of endpoint devices that send and receive information.

2. **Connectivity**

The objective of the IoT Reference Model is for communications and processing to be executed by existing networks.

3. **Edge Computing**

This may involve the following:

- Evaluation of data for criteria as to whether it should be processed at a higher level.
- Formatting & reformatting of data for consistent higher-level processing.
- Expanding/decoding for handling cryptic data with additional context (such as the origin)
- Distillation/reduction for reducing and or summarizing data to minimize the impact of data and traffic on the network and higher-level processing systems.
- Assessment for determining whether data represents a threshold or alert; this could include redirecting data to additional destinations

4. **Data Accumulation**

This level will deal with the following questions:

If data is of interest to higher levels: processing is the first level that is configured to serve the specific needs of a higher level.

- If data must be persisted: Should data be kept on disk in a non-volatile state or accumulated in memory for short-term use?
- The type of storage needed: Does persistency require a file system, big data system, or relational database?
- If data is organized properly: Is the data appropriately organized for the required storage system?
- If data must be recombined or recomputed: Data might be combined, recomputed, or aggregated with previously stored information, some of which may have come from non- IoT sources.

5. **Data Abstraction**

The data abstraction level must process many different things.

- Reconciling multiple data formats from different sources
- Assuring consistent semantics of data across sources
- Confirming that data is complete to the higher-level application
- Consolidating data into one place (with ETL, ELT, or data replication) or providing access to multiple data stores through data virtualization
- Protecting data with appropriate authentication and authorization
- Normalizing or denormalizing and indexing data to provide fast application access

6. Application((Reporting, Analytics, Control)

Mission-critical business applications, such as generalized ERP or specialized industry solutions

- Mobile applications that handle simple interactions
- Business intelligence reports, where the application is the BI server
- Analytic applications that interpret data for business decisions
- System management/control center applications that control the IoT system itself and don't act on the data produced by it.

7. Collaboration and Processes(Involving people and business processes)

The IoT system, and the information it create, is of little value unless it yields action, which often requires people and processes.

Applications execute business logic to empower people. People use applications and associated data for their specific needs. Often, multiple people use the same application for a range of different purposes. So the objective is not the application—it is to empower people to do their work better. Applications give business people the right data, at the right time, so they can do the right thing.

.

C. The OIC Cloud Native Architecture

The OIC cloud-native architecture is based on protocols that support discoverability and connectivity for both local and cloud configurations, supporting a broad range of vertical IoT markets, backed by a formal certification program and the IoTivity open source project.

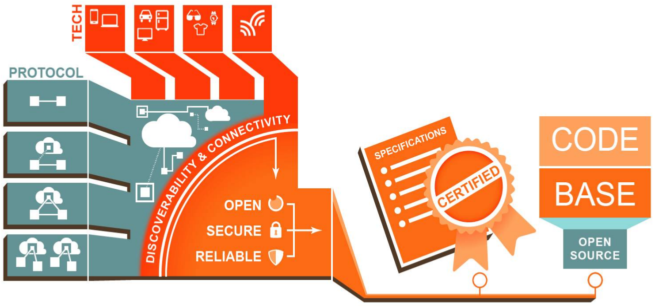


Fig3: The OIC Cloud Native Architecture

D. The Cisco IoT/M2M architecture

The Cisco IoT/M2M architecture is composed of four layers as shown in the figure below.

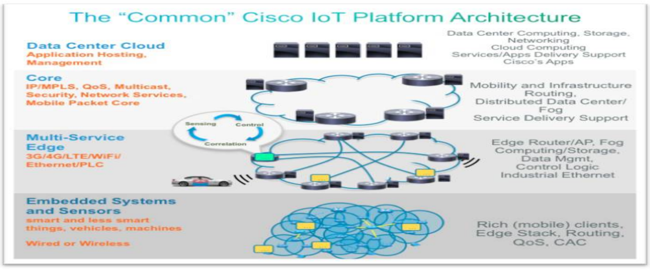

The "Common" Cisco IoT Platform Architecture
Data Center Cloud
Application Hosting, Management
Data Center Computing, Storage, Networking
Cloud Computing
Services/Apps Delivery Support
Cisco's Apps
Core
IP/MPLS, QoS, Multicast, Security, Network Services, Mobile Packet Core
Mobility and Infrastructure Routing,
Distributed Data Center/ Fog
Service Delivery Support
Sensing
Control
Correlation
Multi-Service Edge
3G/4G/LTE/WiFi/ Ethernet/PLC
Edge Router/AP, Fog Computing/Storage,
Data Mgmt,
Control Logic
Industrial Ethernet
Embedded Systems and Sensors
smart and less smart things, vehicles, machines
Wired or Wireless
Rich (mobile) clients,
Edge Stack, Routing,
QoS, CAC

Fig 4:. The Cisco IoT/M2M architecture

1. Embedded Systems Layer

It is comprised of embedded systems, sensors and actuators which are small devices, with varying operating systems, CPU types, memory, etc. Many of these entities are expected to be inexpensive, single-function devices with rudimentary network connectivity, such as a temperature or pressure sensor. In addition, these devices could be in remote and/or inaccessible locations where human intervention or configuration is almost impossible.

These sensors are introduced during the construction phase to collect and monitor data and events. Secondary links will help in cases where the connectivity is lost after the installation teams have left the site.

Additionally, methods must be taken to ensure that the authenticity of the data, the path from the sensor to the collector and the connectivity authentication parameters between the initial installation/configuration of the device, and its eventual presence on the IoT infrastructure cannot be compromised.

2. Multi-Service Edge Layer

The variability in the capabilities of endpoint devices, and their potentially enormous numbers highlight the importance of the multi-service edge in the IoT/M2M architecture. The multi-service edge is multi-modal and supports both wired and wireless connectivity. Even within those two categories, this layer must support many different protocols, such as Zigbee, IEEE 802.11, 3G and 4G, to accommodate a variety of endpoints.

In some cases, the protocols used by endpoint devices may not even have any inherent security capabilities at all. It is imperative for security services to protect these inherently insecure endpoints. Additionally, this layer must be modular to scale to meet growth requirements. The components and services offered within one module should be similar so that additional modules can be added in a short span of time.

3. Core Network Layer

The architecture of the core network layer is similar to the architecture deployed in conventional networks. The function of this layer is to provide paths to carry and exchange data and network information between multiple sub-networks. The main differentiator between IoT and conventional core layers is traffic profile. The IoT traffic and data may be different, for example, unique protocols and variable packet size.

Security services at the core network ensure that the IoT/M2M system as a whole, and has been hardened to protect against threats such as the following:

Man-in-the-middle (MITM) is the means by which the attacker can successfully create a connection between two points and eavesdrop into their conversation by relaying the messages it hears from one peer to the other while also capturing the data.

Impersonation (spoofing) is the means by which an attacker has compromised an identity and thus, through impersonation can send malicious traffic to victim endpoints on the network.

Confidentiality compromise is the means by which the data that is being relayed can be altered by an attacker. Replay attack is the means by which valid data is retransmitted or delayed by an adversary to gain access to an already established session by spoofing their own identity.

4. Data Center Cloud Layer

The function of this layer is to host applications that are critical in providing services and to manage the end-to-end IoT architecture. Again, security services in the data center/cloud network are critical in ensuring that the IoT/M2M system as a whole has been hardened to protect against threats such as ,the Denial of Service (DoS) & Component and endpoint exploitation. The application servers and devices within this layer may also be exposed to buffer overflow and remote code execution attacks if security hardening and best practices are not followed. The threats in these layers, whether DoS, transaction replays, or compromised systems typically can be addressed through established cryptographic mechanisms, provisioning of strong identities with credentials to allow them to authenticate into the network, and with strong policies to affect the appropriate access controls.

E. IDCArchitecture

IDC defines the Internet of Things, as IoT is: "An aggregation of endpoints — or 'things' — that are uniquely identifiable and that communicates over a network without human interaction, using some form of automated connectivity, is it locally or globally."

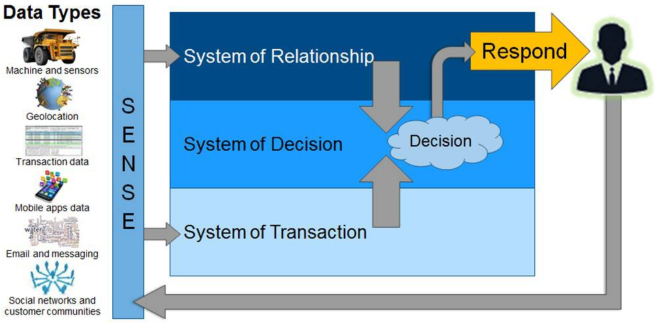


Fig 5 :IDC IoT Architecture

IDC believes that the maturity, widespread availability, and deployment of cloud computing, mobility, and Big Data and analytics are essential to a successful IoT deployment. A cloud environment is important, given that IT directors have to be able to scale their IT infrastructure economically and at speed. IoT sensors create a lot of data that would be worthless without any analytics applied to it so that business outcomes are generated. Finally, given that sensors have to be connected to a network, having a mobile strategy to manage the devices and the applications is the final table stake in an IoT infrastructure world. Using the 3rd Platform elements, the IoT architecture and business model can be viewed through the many "systems" approach. One of the first changes or outcomes from a complete strategy is the nature of business workflow. Companies that used to go to market with a make and sell strategy (where they produced goods and sold them through a traditional channel and the goods were eventually acquired by their customers) have now moved to a completely different model. This new model is driven by the customer who has the ability to interactively drive the supply chain. Here, companies have flipped 180 degrees, and their go-to-market business model is led by a sense and respond strategy whereby they listen (through IoT-gathered data) to their customers. Based on customer behaviors, companies will dynamically change product cycles, features, benefits, suppliers, logistics, and so forth because the IoT sensors across the supply chain have enabled the companies to add new value through social business experiences (see Figure above).

F. WSO2 Architecture

WSO2 is an open source technology company providing service-oriented architecture(SOA) middleware. WSO2 is one of the only vendors that can deliver all components of both architectures that is Event & Enterprise driven. WSO2 is also open source and built to be enterprise grade throughout.

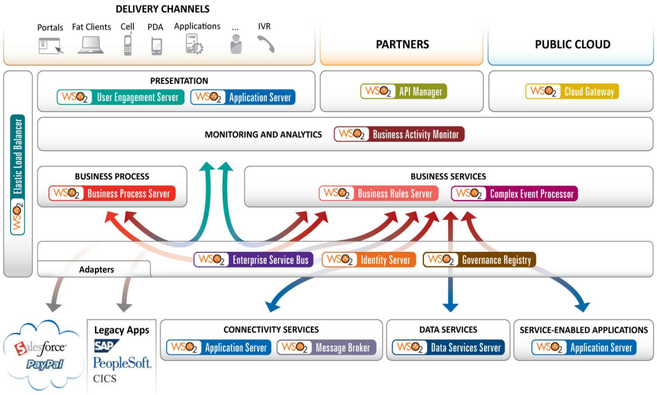


Fig 6 :WS20 Architecture

G.Computing Community Consortium Architecture

The figure below shows the CCC IoT architecture.

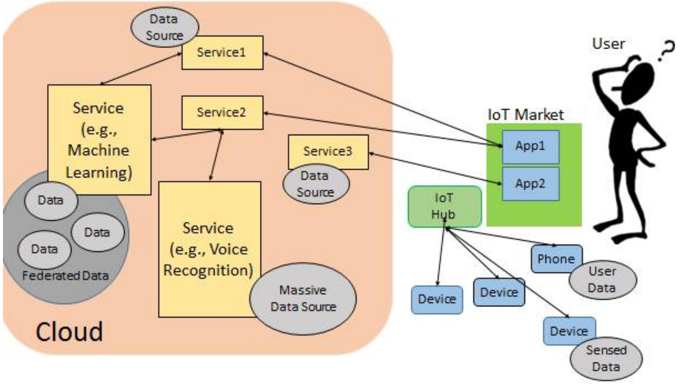


Fig 7: CCC IoT Architecture

The major components of a generic IoT system and how they interact are as discussed below.

- Hardware devices that are able to sense and interface with the physical world.
- Data collected on the behalf of the user by these devices.
- IoT hubs that funnel data from the physical world to the cloud.
- An IoT marketplace with value-added apps that interact with devices and the cloud.
- Services, large and small, that the apps connect to (could be one or more, could be a vertical device-app-service, or could be stratified)
- Varying sizes of data stores, including federated data stores that normalize data from.

IV. CONCLUSION

The study reveals that, while each vendor has their own unique IoT platform visualization, they share a number of similarities. This is not so difficult to understand ,realizing the fact that IoT is the collaboration of people and connected things. On an operational level, collaboration calls for efficient yet flexible processes. On a strategic and tactical level, it is important to empower humans to make the right decisions. This is indeed reflected in most IoT platform visualizations, which depict key software components for

- connecting and managing people so that they can communicate, be informed, decide, and act upon the decisions and/or the information provided.
- enabling the analysis, processing, and storage of information.
- enabling the definition, execution, and monitoring of business processes across different systems
- Connecting and managing things so that they can sense and act.

With no central IoT standards and no real oversight over development, the nearly five billion smart devices as Gartner estimates will be in use by the end of this year are an enticing target for those looking to wreak havoc—or worse.

REFERENCES

1. Towards a definition of the Internet of Things (IoT) Revision 1 – Published 27 MAY 2015, IEEE.
2. How is the Internet of Things like a Trading Floor or StockExchange? BY LOGICLOGICLOGIC ON APRIL 2, 2015.
3. http://blog.bosch-si.com/categories/technology/2014/12/iot-platforms-101/
4. The state of IoT standards: Stand by for the big shakeout By Christopher Null
5. White Paper-Three IT Companies, HDS, Huawei, and IBM,Three Different IoT Paths --Vernon Turne
6. JD Edwards EnterpriseOne Internet of Things Orchestrator--ORACLE WHITE PAPER JULY 2015
7. Planning for Industrial Internet of Things By Greg Gorbach,Arc Strategies
8. Systems Computing Challenges in the Internet of Things Rajeev Alur, Emery Berger, Ann W. Drobnis, Limor Fix, Kevin Fu, Gregory D. Hager, Daniel Lopresti, Klara Nahrstedt, Elizabeth Mynatt, Shwetak Patel, Jennifer Rexford, John A. Stankovic, and Benjamin Zorn --- September 22, 2015
9. IoT-A Reference Model september 12, 2015, Smart Science
10. Securing the Internet of Things: A Proposed Framework ,Cisco Whitepaper
11. The Open Interconnect Consortium and IoTivityWhite Paper
12. ZigBee 3.0 – The Open, Global Standard for the Internet of Things December 2, 2014