Technical Architecture & stacks

Open source Framework

Date	19 September2022
Team ID	PNT2022TMID43285
Project Name	IoT Based Safety Gadget for Child Safety Monitoring and Notification
Maximum Mark	2 Marks

1. **Physical/device layer.** This comprises the sensors, actuators and other smart devices and connected devices that comprise the physical layer and device layer. These smart devices either capture data (sensors), take action (actuators) or sometimes both.
2. **Network layer.** This comprises the network devices and communications types and protocols (5G, Wi-Fi, Bluetooth, etc.). Although many IoT architectures rely on general-purpose network layers, there is an increasing trend to move to dedicated IoT-specific networks.
3. **Data/database layer.** This also includes the database platform layer. There are a range of databases used for IoT architectures, and many organizations spend a fair amount of time selecting and architecting the right IoT databases.

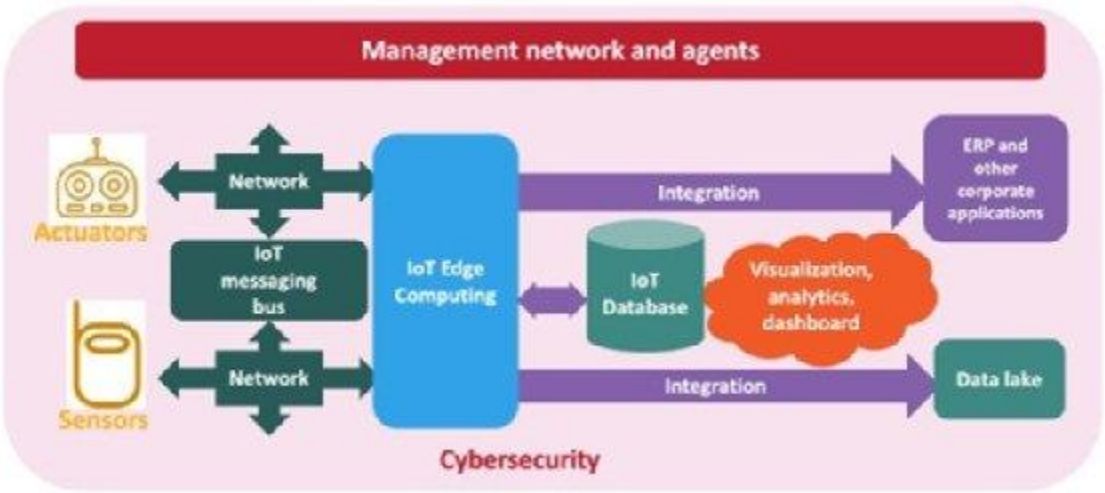
Together, the physical layer/device layer, network layer and data/database layers comprise the infrastructure component discussed above.

4. **Analytics/visualization layer.** This layer comprises the analytics layer, visualization layer and perception layer. In essence, this layer's focus is on analyzing the data provided by IoT and providing it to users and applications to make sense of.
5. **Application/integration layer.** This is the layer of applications and platforms that integrate together to deliver the functionality from the IoT infrastructure to the business. In other words, the application layer, platform layer and integration layer are what provide the business value from the IoT

infrastructure. The processing layer and business layer are all part of the larger application/integration layer.

6. **Security and management layer.** As the name implies, this layer encompasses both the security layer and the management layer. Strictly speaking, this is not a *layer* as it has connections with all the other layers to provide security and management. But it's an important component that's worth considering at every layer.

These layers go from bottom to top in a fashion similar to the Open Systems Interconnection model, which was the original source of the layering concept. (See Figure 3 below).



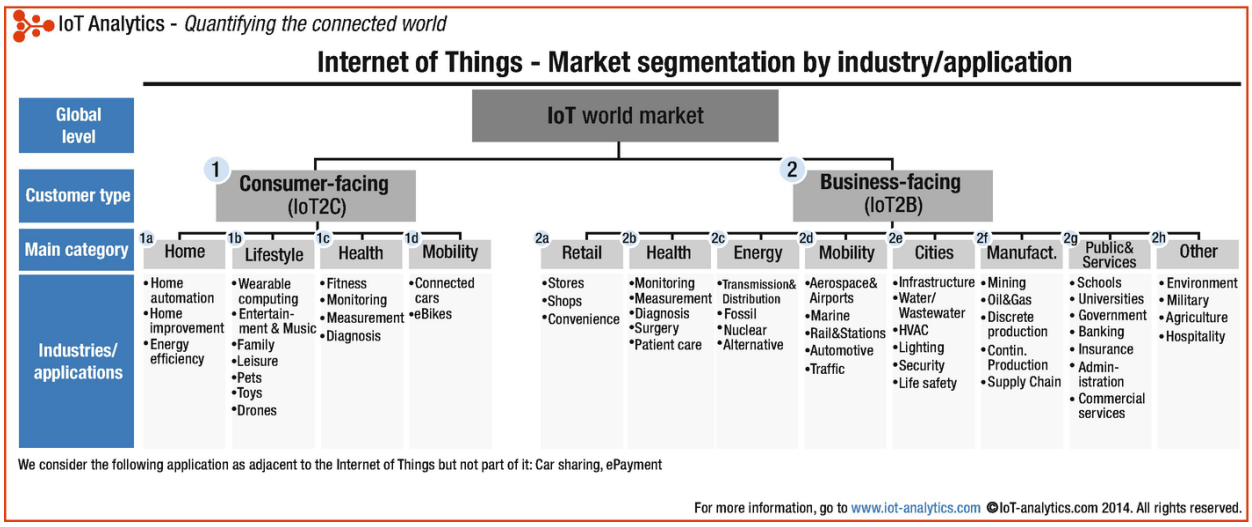
NEMERTES RESEARCH

Figure 3: An overview of the IoT architecture model

Conclusion and recommendations

Enterprise IT, OT and IoT technology professionals should develop IoT projects and initiatives based on a consistent architecture. That doesn't mean using the exact same tools and technologies for every project, but rather making sure every component is properly instantiated for the specific project, and that technology professionals have thought about all the layers, including the network layer,

perception layer, processing layer, physical layer, gateway layer, platform layer, device layer, business layer, security layer and sensor layer.



the components of an IoT architecture

At a high level, the components involved in an IoT architecture include four key components. (See Figure 1 below).

- The **applications and analytics component.** This is the piece that processes and displays information collected via IoT. It includes analytics tools, AI and machine learning and visualization capabilities. Technologies for this component range from traditional analytics and visualization packages, such as R, IBM SPSS and SAS, to specialized IoT tools and dashboards from cloud providers, such as Amazon, Google, Microsoft, Oracle and IBM, as well as application suite vendors, including SAP and Salesforce.
- The **integration component.** This is the component that ensures that the applications, tools, security and infrastructure integrate effectively with existing companywide ERP and other management systems. Providers include the aforementioned software and cloud players, as well as a range of open source

and middleware providers, such as Oracle Fusion Middleware, LinkSmart, Apache Kafka and DynThings Open Source IoT Platform.

- The **security and management component.** IoT security includes securing the physical components of the system via firmware and embedded security providers, such as Azure Sphere, LynxOS, Mocana and Spartan. Traditional security vendors, such as Forescout, Symantec and Trend Micro, also offer packages that focus specifically on securing IoT.
- The **infrastructure component.** This includes physical devices -- IoT sensors, which capture information, and actuators, which control the environment. It also includes the network on which the sensors or actuators reside. Typically, though not always, this is a wireless network, such as Wi-Fi, 4G or 5G.