Research online Publishing www.ronpub.com

Open Access

Open Journal of Internet of Things (OJIOT)
Volume 5, Issue 1, 2019
http://www.ronpub.com/ojiot
ISSN 2364-7108

Towards a Large Scale IoT through Partnership, Incentive, and Services: A Vision, Architecture, and Future Directions

Gowri Sankar Ramachandran, Bhaskar Krishnamachari

USC Viterbi School of Engineering, University of Southern California, 3650 McClintock Ave, Los Angeles, CA 90089, USA {gsramach, bkrishna}@usc.edu

Abstract

Internet of Things applications has been deployed and managed in a small to a medium scale deployments in industries and small segments of cities in the last decade. These real-world deployments not only helped the researchers and application developers to create protocols, standards, and frameworks but also helped them understand the challenges associated with the maintenance and management of IoT deployments in all kinds of operational environments. Despite the technological advancements and the deployment experiences, the technology failed to create a notable momentum towards large scale IoT applications involving thousands of IoT devices. We argue the reasons behind the lack of large scale deployments and the limitations of contemporary IoT deployment model. In addition, we present an approach involving multiple stakeholders as a means to scale IoT applications to hundreds of devices. Besides, we argue that the partnership, incentive mechanisms, privacy, and security frameworks are the critical factors for large scale IoT deployments of the future.

Type of Paper and Keywords

Visionary Paper: *IoT, applications, scalability, smart city, multi-stakeholder, data economy*

1 Introduction

Internet of Things technology is starting to be deployed in real-world environments, including cities [44, 33], industries [36], and homes [38]. Such real-world deployments consist of sensors and actuators to remotely monitor and manage the environment. Computation and communication are the critical building blocks of the IoT applications. Several research and development efforts in the last decade lead to the creation of a wide number of protocols and frameworks to meet the communication, computation and sensing demands of the IoT applications.

The technological advancements made in the last decade enabled the application developers to deploy and manage applications only at small to a medium scale involving tens of IoT devices [20, 42]. Scaling IoT deployments to hundreds of devices still remains a challenge due to a) the heterogeneous nature of hardware devices, networking protocols, and peripherals including sensors and actuators, b) the management and maintenance complexity as the devices are susceptible to faults and failures and may require periodic maintenance to replace battery or to calibrate sensors, c) the technological limitations of the

This paper is accepted at the *International Workshop on Very Large Internet of Things (VLIoT 2019)* in conjunction with the VLDB 2019 conference in Los Angeles, USA. The proceedings of VLIoT@VLDB 2019 are published in the Open Journal of Internet of Things (OJIOT) as special issue.

single stakeholder deployment model since designing applications assuming there is only one administrator (stakeholder) is one of the fallacies in designing distributed systems [29].

In this vision paper, we argue that the single stakeholder deployment model poses the most significant limit on the scalability of the IoT. As an alternative, we present a multi-stakeholder IoT deployment model by decomposing the functionalities of the IoT network stack into a set of services and enabling the community members, including commercial organizations to provide the different services. Following our multi-stakeholder deployment model, various entities can deploy, manage, and offer different sensing, routing, and computation services for building large scale IoT applications. Application developers are only required to subscribe to the necessary services, and in some cases, he/she may have to buy pre-configured hardware devices to compose an application rapidly.

Furthermore, we describe how multi-stakeholder deployment model improves the scalability and illustrates the benefits of such a deployment model through the ongoing commercial and research efforts. Besides, we present the open research challenges in operating in a multi-stakeholder setting including the need to introduce incentive, issues around data ownership, trust, and privacy, and the need to organize and adopt a common set of standards to increase interoperability. Lastly, we present the critical building blocks of a multi-stakeholder IoT deployment model to encourage the IoT enthusiasts and application developers to move towards a large-scale and multi-stakeholder IoT applications.

The rest of the paper is structured as follows: Section 2 presents the architecture and the different layers of the IoT application. The different factors that limit the scalability of the single stakeholder deployment model are discussed in Section 3. The advantages of reusing sensors and communication services are presented in Section 4. Section 5 presents the advantages of multi-stakeholder deployment model. Examples of multi-stakeholder efforts are presented in Section 6. Section 7 presents some of the open challenges in developing a multi-stakeholder deployment model. The key building blocks of a multi-stakeholder IoT architecture is discussed in Section 8. Lastly, Section 9 concludes the paper.

2 Architecture of Single Stakeholder IoT Deployment Model

Contemporary IoT applications are developed using a three-layer architecture (see Figure 1). The first layer represents the end-devices or "connected things", which are IoT hardware platforms equipped with sensors and actuators for monitoring and controlling the operational environment. The data collected from the IoT hardware devices are reported to either the edge server or the cloud infrastructure depending on the application requirement. The decision to process the data on the edge or the cloud depends on the latency and the processing demands of the application. Typically, the applications that require faster response use the edge servers due to their proximity to the IoT hardware devices, and the applications that demand long term storage or the execution of computationally intensive data analytics algorithm use the cloud infrastructure. Some applications use the combination of edge and cloud infrastructure to handle various application services.

2.1 Connected Things

Hardware devices are central to IoT applications. Data processing, storage, interfacing, and in some cases, the communication capabilities of devices depend on the onboard resources. Internet Engineering Task Force's (IEFT) draft on "Terminology for Constrained-Node Networks" classifies the IoT devices into three different classes based on the program (flash) and code (RAM) memory sizes [17].

Class 0 devices are severely constrained with extremely limited resources for processing and storage. The lack of resources makes these devices less suitable for computation-intensive applications such as wireless security protocols that require significant computation and storage resources for encryption and decryption operations. Besides, class-0 devices do not connect directly to the Internet due to their limited radio capabilities, and in all cases, the devices in this category rely on a gateway or a proxy server for Internet connectivity.

Class 1 devices have limited constraints, and they have enough computation and storage resources for running a lightweight network stack. Devices in this category are capable of supporting messaging protocols such as CoAP [35] and MQTT [2] besides enabling IP-based communication. Lastly, Class 2 devices are less resource constrained and are capable of running a complete network stack similar to the one used in notebooks and laptops. Typically, class-2 devices are used as a communication gateway for enabling Internet-connectivity to other resource-constrained devices.

Ownership of Sensor Networks: IoT applications in the last decade were owned and managed by a single organization. Thus, the organization deployed their IoT devices to achieve only one application goal. In the case of Great Duck Island deployment [20], the devices measured the temperature and humidity of bird nests.

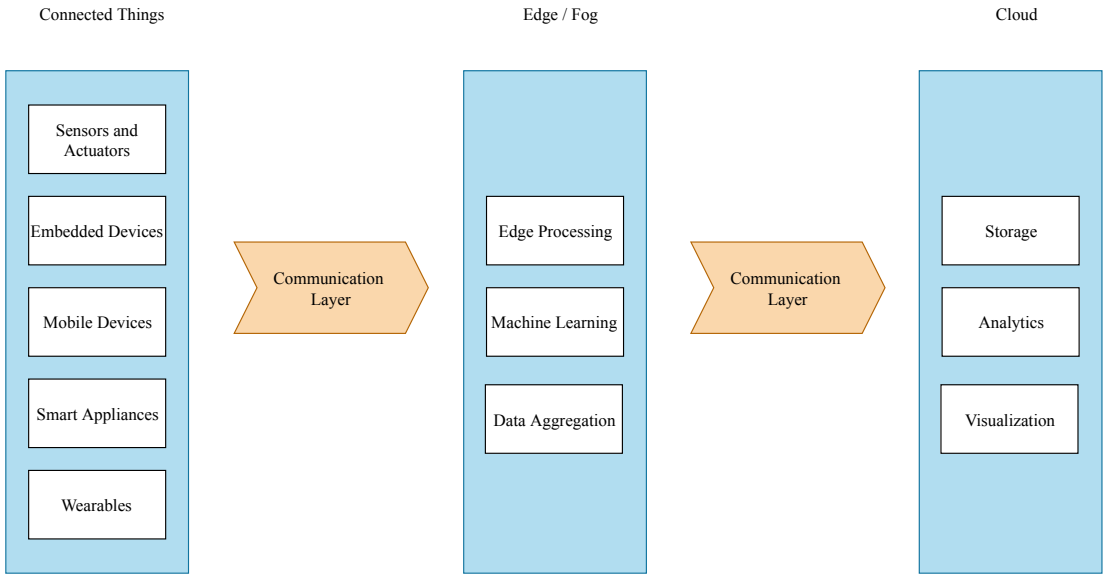

Figure 1: Architecture of single stakeholder IoT deployment model

However, the same data can be used by researchers studying climate change. In the single stakeholder deployment model, the application is developed with a single goal in mind, and it may not be easy to open up the infrastructure to support multiple applications.

2.2 Communication Support for the IoT

From Figure 1, it is clear that the IoT end-devices require communication support to report the data to the remote edge or cloud infrastructure. Depends on the communication modalities followed by the IoT end-devices, the IoT end-devices connect to a centralized gateway to transport the data to the remote edge or cloud infrastructure. Table 1 lists the contemporary wireless communication standards that are widely employed in IoT application deployments. Each communication standard follows a different network topology and physical layer technology to enable device-to-device communication. Moreover, the wireless communication range of the physical layer (i.e., radio) determines the effective range, which means large scale IoT deployments with hundreds of devices have to choose the right physical layer technology and the network topology for wireless communication.

From Table 1, it is evident that the communication standards themselves define who are the stakeholders and what is their role in IoT application deployments. Most importantly, all the communication standards do not follow a single stakeholder deployment model. Therefore, the application developers are required to assess the characteristics, operational, and maintenance costs of different communication technologies before deciding on a communication standard for the IoT applications. Note that the single stakeholder deployment model may become challenging to manage when the application consists of hundreds to thousands of IoT devices, but it enables the organization that owns and operates the IoT application and the hardware infrastructure to easily reconfigure the network infrastructure to meet the evolving demands of the IoT applications.

Ownership of Communication Infrastructure: Typically, the communication support for the IoT deployment is provided through either a short range or long range radio transceiver. Real-world applications in the last decade heavily depended on short-range radios because of their low power consumption. These deployments were owned and managed by a single stakeholder to meet the demands of a single application. However, the LPWAN technologies introduced an alternative communication modality for the IoT deployments. The long-range communication support in the order of hundreds of meters coupled with their low power consumption made them an excellent alternative for IoT deployments. Besides, the LPWAN technologies consisted of a gateway which was deployed either by a commercial provider or IoT enthusiasts to provide communication services for the IoT application [4, 3, 12]. Therefore, the ownership model is slowly changing on the communication front, and the future IoT deployments have to coordinate

Table 1: Characteristics and the stakeholder (ownership) model of contemporary IoT communication technologies (Note that the hybrid in the table refers to a deployment model in which the communication infrastructure can be deployed either by the organization that implements the application or leverage the existing communication infrastructure made available by other organization. The single stakeholder refers to a deployment model where the communication infrastructure is deployed and managed by the same organization that runs the application. Lastly, the multiple stakeholders refer to a deployment model in which the communication infrastructure is provided by a third-party, which means the application developers are required to buy a subscription from the service provider before deployment.)

Communication Standards	Topology	Communication Range of the Physical Layer(s)	Stakeholder Involvement
IEEE-802.11 [7]	Star (Uses a centralized gateway)	Tens of meters	Hybrid
IEEE-802.15.4 c[11]	Mesh and Tree (Devices connect to Internet via one or more devices)	Tens of meters	Single Stakeholder
IEEE-802.15.4e [40]	Mesh (Devices connect to Internet via a central network manager)	Tens of meters	Single Stakeholder
Bluetooth [21]	Peer-to-peer and mesh	Tens of meters	Hybrid
LoRaWAN [8]	Star	Hundreds of meters	Hybrid
3G/4G/5G [6, 1]	Star	Hundreds of meters	Multiple Stakeholders

with the communication service providers to meet its application demands.

2.3 Edge Server

IoT applications employ edge servers to reduce the response time of the latency-sensitive applications by processing the data close to the data source. The physical location and the ownership of the edge server are loosely defined in the infrastructure. Majority of the edge computing frameworks in the literature [34, 28, 37] assume that an edge server is tightly integrated with the communication gateway (see Table 1) to realize edge computing. In such a deployment model, the organization that runs the application also manages the edge server, which essentially means that the organization can upgrade the edge server in case the application requires more computation resources at the edge. However, the telecom operators [14, 41] and CDN providers are presenting an alternative model wherein the elastic edge servers are readily available for the large scale IoT applications. Application developers may have to purchase a combined subscription for bandwidth and edge computing to build flexible and scalable applications for edge computing.

2.4 Cloud Server

Cloud infrastructure allows the application developers to leverage powerful computation and storage platforms along with an extensive collection of services, including data analytics and visualization. Applications leveraging the cloud infrastructure typically have to rely on platform as a service providers to build cloud-based IoT applications. Applications using the cloud platforms are already operating in a multi-stakeholder environment, and the application developers are already trusting the cloud service providers when computing and storing data at a cloud infrastructure.

3 Limitations of Single Stakeholder IoT Deployments

3.1 Management Complexity of Connected Devices and Communication Infrastructure

IoT deployments with hundreds of devices are harder to manage as each device in the network requires both computation and communication resources. For the devices to report their sensor data to a remote edge or cloud infrastructure, the application developers have to provide communication resources and needs to ensure that the devices are actively reporting the data. Besides, the literature [9] reports that wireless communication

expends a significant amount of energy on IoT devices. Therefore, the battery operated IoT devices require regular battery replacement to keep the devices active.

Similarly, applications developed with a single application goal reports data following a custom protocol, when the same data is needed for other applications, the application software may have to be reconfigured. A single purpose application limits the utilization of the hardware devices.

Application management becomes a challenging problem when the application network consists of hundreds to thousands of IoT devices.

3.2 Rapid Evolution of Technology

A large scale IoT deployment requires a collection of IoT hardware devices, sensors, actuators, communication support, edge, and cloud infrastructure. The hardware and the software technology for the IoT is rapidly developing, which means the technology adopted by an IoT deployment needs to be upgraded regularly to reduce the operational costs while securing the infrastructure against malicious attacks. Organizations hesitate to invest heavily on large scale infrastructure because of this constant evolution [19]. An investment made for a single application may only be useful until the arrival of novel hardware technologies and innovative solutions.

Technology becomes obsolete very quickly due to the rapid evolution of technology.

3.3 Limitations of Contemporary Technologies

IoT deployments employ a wide array of network protocols, operating systems, and hardware devices. Standards are being developed and maintained for all the layers of the protocol stack. However, not all the operating systems and network stacks are uniform and interoperable. Due to the lack of interoperability, the hardware devices and software configurations followed for a given application may not work with other applications or other protocols. Although application developers can write adapters and other gluing code to enable interoperability, this form of application development becomes harder to manage when a new standard emerges, or there is a change in application requirement.

Besides, different devices in the network produce different classes of traffic, ranging from periodic reporting of sensor data to non-periodic unpredictable traffic from PIR or RFID sensors. Provisioning bandwidth resources for periodic traffic is easy due to their predictable transmission behavior, but it becomes challenging for applications with unpredictable transmission behavior [27]. IoT devices may not be able to reliably report their data to remote infrastructure if they do not have sufficient bandwidth resources and allocating bandwidth is a challenging problem when the application traffic is heterogeneous.

Besides, the majority of the low-power wireless networking solutions are tailored for upstream communication, which means the devices are not easily accessible for reconfiguration purposes. Provisioning bandwidth for downstream communication reduces the throughput for upstream communication since the devices share the communication channels and the radio hardware for both upstream and downstream communication.

To maximize the return-on-investment, application developers need to understand the limitations and the effectiveness of the network protocols and physical layer technologies.

4 Increasing Utility and Return-on-Investment

Figure 2 shows the application model of single stakeholder IoT deployments wherein each vertical application is deployed to achieve a single goal. For example, the air quality monitoring application uses temperature, particle measurement, humidity, and gas sensors to acquire air quality data and use the sensed information to adjust the HVAC settings. In the same deployment site, a fire detection and response application deploy similar sensors to detect and respond to fire. However, the sensors deployed and managed by the air quality application can be used by the fire detection application to increase the utility and the return on investment. At the same time, the communication infrastructure deployed by one of the applications can easily be shared with other applications. These deployments show that the utility of the IoT infrastructure can be maximized by leveraging the existing resources for multiple applications. Moreover, developing and designing IoT applications following such a model enable the application developers to focus only on either gathering the data or connecting with the existing communication infrastructure, instead of deploying and managing the entire ecosystem.

5 Multi-Stakeholder Model for Large Scale IoT Deployments

The literature either discusses the involvement of multiple stakeholders [10, 16] or motivate the need to involve multiple stakeholders to increase the utilization of IoT deployments [19]. Gubbi *et al.* [10] classifies the IoT applications into four different categories as home, enterprise, utility, and mobile and further explains

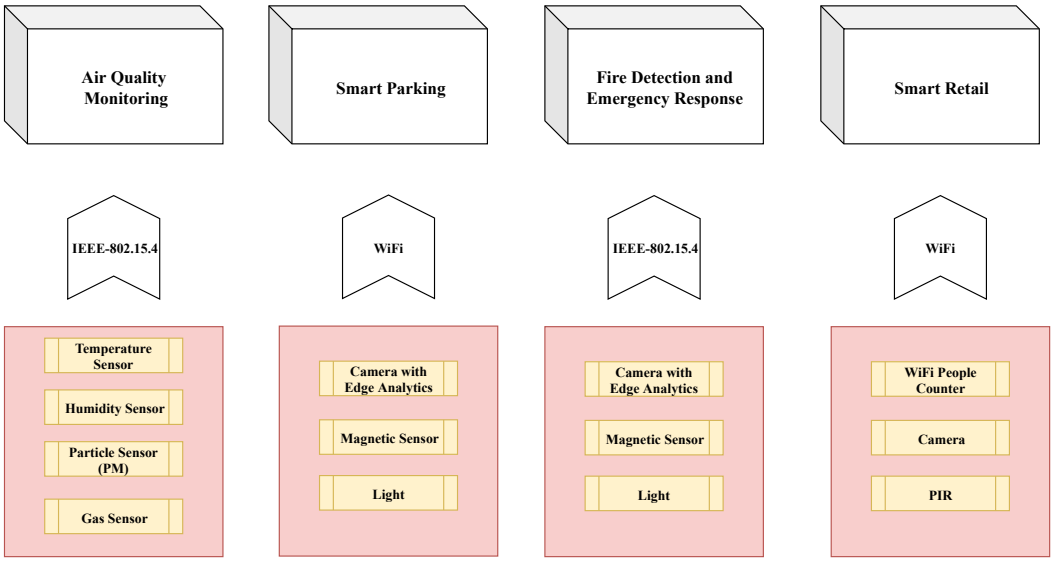

Figure 2: Application model of single stakeholder applications

the deployment and data ownership models followed by various IoT applications. The involvement and collaboration of multiple stakeholders are identified as one of the research challenges for future IoT applications [10]. Saarikko *et al.* [30] motivates the need to partner with multiple stakeholders to increase the business potential and the large scale adoption of IoT. Furthermore, Saarikko *et al.* [30] states that "the IoT is not a homogeneous concept or paradigm, but rather a buffet of possibilities from which each actor can peruse and assemble an approach that is right for their strategic interests and business requirements". Existing literature presents a strong case for multi-stakeholder deployments but does not present any architectural elements of such an application model. Our work introduces the building blocks of a multi-stakeholder IoT model.

5.1 Service-Driven IoT Deployments

From the previous section, it is clear that the single stakeholder deployment model is harder to maintain and manage when the application network consists of hundreds of devices. We suggest a service-driven deployment model involving multiple stakeholders providing various services for the IoT applications. Services in the context of IoT application refers to routing, sensing, computation, analytics, among other things. Enterprise applications have been employing SaaS model [39] for serving a large user base, wherein the organization providing the service manages the software services. Similarly, we propose managed services for the IoT applications to reduce not only the management complexity but also the deployment complexity. The application developer is not required to deploy his/her infrastructure for communication, sensing, computation, among other things; instead, they can compose an application by combining multiple services. IoTMaaS [15] is an application composition model wherein the applications can be created using heterogeneous devices and services through a standardized set of interfaces.

5.2 "Pay-and-Consume" Model

Component-based software engineering decomposes the application functionality into a set of components, which enable the application developers to reuse the components in multiple applications to minimize the development overhead while increasing the flexibility [13]. Following a similar model, the community members including telecommunication companies, city administration, and other IoT enthusiasts can either develop their own IoT service for sensing, computation, communication, and analytics functionalities or buy commercial-off-the-self hardware devices and expose it to the application developers in the form of platform-as-a-service. For such a deployment model to be successful, the service providers should be given an incentive. Application developers can purchase the desired services from the service providers and compose an IoT application. Such a model increases the utility of the hardware devices since multiple

applications can be developed using a given service (or a hardware platform), whereas, in a single stakeholder deployment model, the IoT infrastructure is not made available to other organizations. Therefore, exposing the devices and as well as the infrastructure as services for the application developers increases the utility and the return-on-investment.

5.3 Plug-and-Play Hardware Technology

Pham *et al.* [23] presents the performance evaluation results of widely used IoT hardware platforms. From the evaluation results shown in [23], it is clear that the platforms such as TelosB and MicaZ were capable of supporting only low data rate applications, but a significant effort is needed to configure and manage the network protocols.

Consider a scenario where a large industry interested in adopting IoT technology to make informed decisions about their business processes. Such deployments typically start at a single site and then expanded to more sites based on the effectiveness. Deploying a hardware platform with fixed hardware for computation, sensing, and communication may reduce the return on investment if the hardware technology fails to meet the application demands or in some cases, the platform may become obsolete quickly. However, a plug-and-play hardware platform would enable the industry to expand the capabilities of the hardware platform by integrating new hardware module for communication, computation, and sensing [43, 31].

5.4 Uberization of IoT

The Uber model of car renting enable the vehicle owners to gain monetary benefit by sharing their vehicle with the community through a mobile application. Through this model, the vehicle owners can use their vehicles for both their personal use and as well as serving the Uber customers. When the vehicles are shared through the "Uber" marketplace, the vehicle owners are gaining an incentive based on the service they provide to the community members. Adopting a similar model for the IoT hardware devices would enable the device owners and IoT enthusiasts to share their IoT devices and wireless communication infrastructure for providing sensing, actuation, and routing services. For their contribution to a large scale and multi-purpose IoT application, they would receive an incentive. The I3 data marketplace presented in Section 6.1 is an excellent example of this model.

6 Examples of Multi-stakeholder Efforts

Many development efforts are already moving towards a multi-stakeholder deployment model. In this section, we will present some of the ongoing efforts in this area.

6.1 I3 Data Marketplace

Krishnamachari *et al.* [18] presents I3 data marketplace for smart cities. The I3 platform enables the device owners to monetize their sensor data. Application developers can build IoT applications by paying for a data product. This system is based on the hypothesis that properly motivated individuals will contribute sensor data to a managed IoT marketplace that will make data from different owners available to different application developers to create value for end users. If developers were to compensate device owners for the use of their data, an ecosystem could be created where data owners compete to increase the value of their data to attract more applications. I3 data marketplace focuses on designing a marketplace where device owners, application developers, and data brokers can come together to form an ecosystem that goes significantly beyond today's homogeneous vertical deployments. Figure 3 shows how the application developers can use the infrastructure or the data source provided by the edge devices through the I3 marketplace platform for developing innovative IoT applications.

6.2 Nodle

Nodle [22] is a commercial community-driven networking platform for the IoT. Nodle enables the IoT devices to leverage the Bluetooth connection provided by smartphones to relay the data to the Internet. Smartphones act as a hub for the IoT devices, and the phones that are part of the Nodle ecosystem are rewarded based on the service they provide to the IoT end devices. One of the unique features of Nodle is that smartphones can relay IoT packets from all over the globe, providing global roaming support for the networking hub.

6.3 5G network slicing

Applications in the area of vehicular IoT and smart cities consist of an extensive collection of sensors and actuators with heterogeneous QoS requirements. 5G network slicing efforts is already dividing the spectrum into several sub-bands to satisfy the QoS requirements of the mobile applications [32]. Application developers can subscribe to 5G services based on their bandwidth requirement. Each application would receive a dedicated

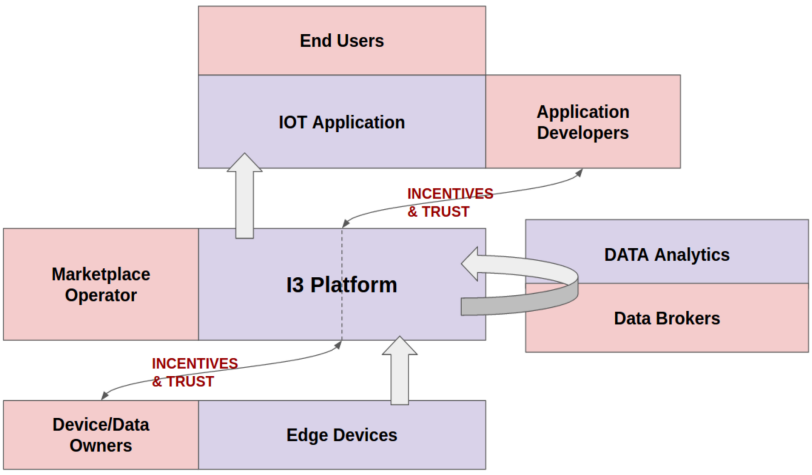

Figure 3: High-level overview of I3 data marketplace [18]

virtual resource for handling its wireless communication demands. Latency-sensitive applications can be isolated from other apps to ensure real-time response for vehicular IoT applications.

6.4 Adoption of Cloud Platforms

IoT and enterprise applications are starting to rely on cloud computing for data analytics, visualization, storage, and for many other software services [5]. In this model, the application developers are already connecting their custom on-premise application infrastructure to a remote cloud infrastructure through standardized APIs. The managed services provided by the cloud platforms enable the organizations to easily scale their application load without having to manage or modify the computation and storage resources on the cloud platform. Organizations are paying cloud providers based on their resource usage, including computation and storage. This model already shows that the corporations are willing to migrate to the infrastructure provided and managed by third parties and interoperate with organizations outside their trust boundaries.

7 Research Challenges and Open Problems in Moving to a Multi-stakeholder Model

7.1 Need for incentive mechanisms

The infrastructure deployed for one application can be useful for other applications, but the contemporary architectures are tightly built to meet the demands of a single application. A sustainable incentive mechanism to the infrastructure owner could encourage the owner and community members to share their infrastructure and as well as the sensor data. It is important to define the role of different stakeholders in the incentive-driven IoT architecture since the multi-stakeholder systems naturally cross economic self-interest boundaries. There is also a need to price services based on the quality of service.

7.2 Dynamic Pricing and Payments

Related to the above point, where the incentives are monetary, it is of importance to enable a wide range of pricing policies for data - from simple static models to dynamic pricing based on demand to auction mechanisms for price discovery in the case of asymmetric, incomplete information. It is also of interest to identify the most convenient way to incorporate payment processing into the framework, such as through the use of price-stable, low transaction fee crypto-currencies. One of our prior work, SDPP [24], presents a payment protocol for the Internet of Things to enable IoT devices to exchange data with other application developers in return for an incentive.

7.3 Privacy Concerns

The multi-stakeholder model enables the infrastructure owners to sell their service to one or more buyers. From the seller's perspective, it is important to ensure that his privacy is protected when selling services to buyers. Besides, the service providers should be allowed to set rules on who can consume the service, and

how the service should be consumed. The platform should, therefore, provide support for privacy protection and contract management when dealing with service providers and consumers.

7.4 Trust and Reputation

The sellers' needs to ensure that their service or the hardware infrastructure are not misused by the consumers, while the buyer of the service needs to trust the service provided by the software or hardware infrastructure is reliable since the applications are composed by connecting multiple services. How can we integrate a trust management framework to a multi-stakeholder IoT architecture? This includes both reputation mechanisms where buyers and sellers can rate each other similar to other online marketplaces for goods and services, as well as exploring the integration of or extension to decentralized trust mechanisms such as distributed ledgers and blockchain technologies.

7.5 Security

Being centralized for each community in its present form, a multi-stakeholder infrastructure may suffer from vulnerability to denial of service - it will be important to incorporate state of the art approaches to deal with this. The architecture will also need to ensure confidentiality of data, possibly through the use of transport layer security mechanisms, and new research may be required to provide efficient, secure computing mechanisms such as partial homomorphic encryption or the use of trusted computing platforms.

7.6 Interoperability

How to coordinate data movement across all the layers, using common protocols and standards for data, networking, and computation, including PHY/MAC/routing/transport/application layers of the stack, usage and access policies, micropayments, smart-contracts, computation specification, QoS, etc.

7.7 Identity Management

In a single stakeholder scenario, all the application developers and the administrators are part of the same organization and follow the protocols set by that organization. When a number of stakeholders provide different IoT services, it is important to maintain a common identity across the entire platform for each of the service providers as this would enable the different members to rate each other and follow the policies and regulations set by the governing body.

7.8 Governing Authority

Since the application developers can compose an application by buying services from different parties, there is no single authority for managing the entire ecosystem or setting policies and regulations for the service providers. A decentralized governing mechanism may be desired to regulate the behavior of the multi-stakeholder ecosystem. For example, Krishnamachari *et al.* [18] presents a consortium model for managing the I3 data marketplace wherein many organizations come together to create common standards and usage policies for the device owners and application developers.

8 Building Blocks of a Multi-stakeholder IoT Architecture

Figure 4 shows a reference architecture, including the building blocks of a multi-stakeholder IoT deployment model. Remember that single stakeholder deployments are typically maintained and managed by administrators and application developers belong to a single organization. Therefore, the application components were developed and configured by trusted members within the organization's trust boundary. We advocate for a multi-stakeholder deployment model to increase the scalability and to minimize the deployment and the maintenance overhead. However, the multi-stakeholder model involves different stakeholders from various organizations, which means there is a need to guarantee trust, security, privacy, and a set of common standards and regulations for the ecosystem members. In this section, we present a reference architecture of a multi-stakeholder deployment model and explain its key building blocks.

Identity Management: As discussed in Section 7.7, the service providers are not part of a single organization. For example, the sensing service provider may operate with a networking service provider to report data to a visualization service provider serving at the cloud platform. From Figure 4, it is clear that the sensing and the application services are running at the "connected things" layer while the visualization service is running at the cloud platform. Without having a common identity management platform, it becomes difficult for the application developers to trust the different service providers and rate them since they don't belong to a single organization in our multi-stakeholder setting. Besides, the service providers that are part of the ecosystem may register their services in the registry to let the application developers search and discover the desired services. Such operations require an identity on the ecosystem.

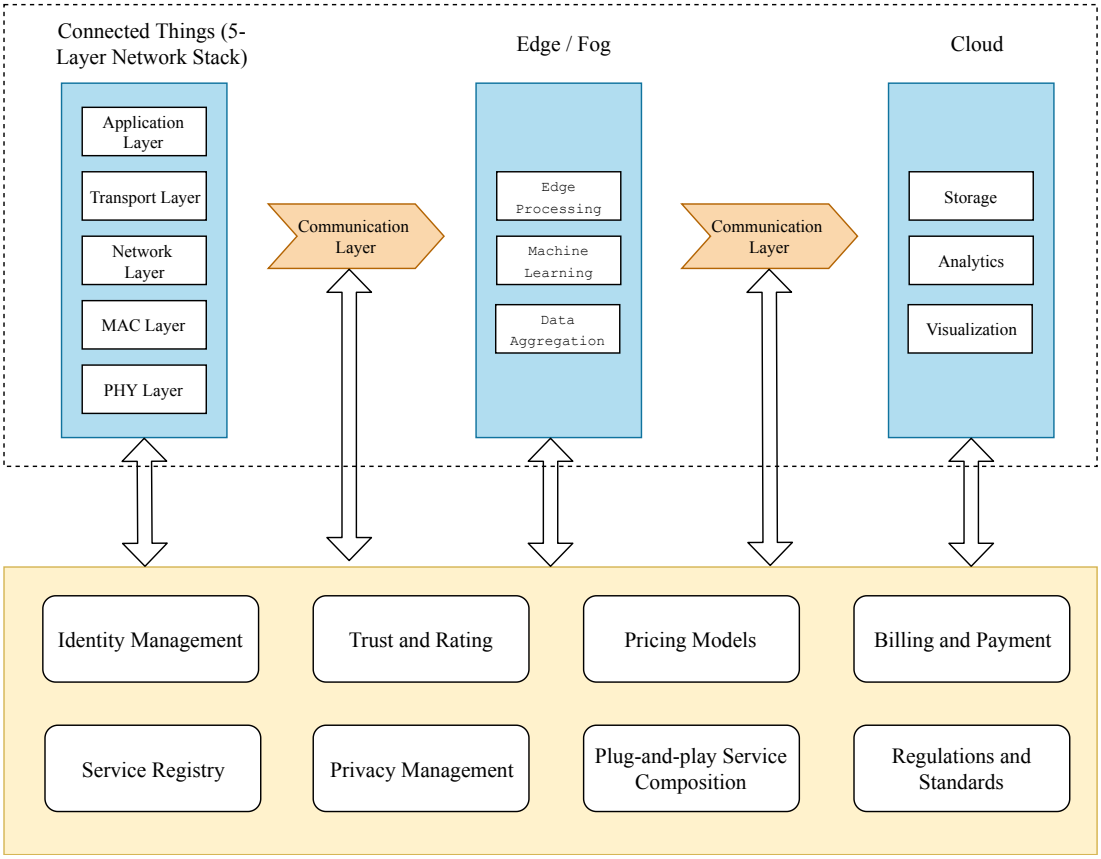

Figure 4: Building blocks of a multi-stakeholder IoT architecture

Trust and Rating: Since the application developers are composing applications by combining services from various stakeholders, it is essential to ensure that the providers are behaving honestly and are not cheating the application developers. Using a rating scheme, the application developers and the service providers can rate each other based on their experience.

Pricing Models: Allowing the service providers to set the price for different services may lead to an unregulated market with providers fixing unreasonable prices. Therefore, a pricing model should be developed to help the service providers select a price for their service. The service price may be adjusted based on the QoS requirement or the reputation of the service provider.

Billing and Payment: Modern day cloud platforms consist of a registration process during which the user enters his/her credit card information. After the registration phase, the user can choose the desired service, and the platform charges the user based on resource usage. A similar mechanism may be desired for the application developers to easily compose and pay for the services from one common platform rather than logging into multiple payment platforms to pay for different services.

Service Registry: Marketplaces such as Amazon and eBay list the products based on their category, price, etc. Similarly, a service registry with information about the location, price, rating, and other relevant metadata is needed to help the application developers. Upon discovering the required services, the application developers can easily compose an application through a plug-and-play composition framework (see below).

Privacy Management: Service providers and the application developers are exchanging various information, including location and other sensitive information during the application composition stage. To protect and respect the privacy of the different stakeholders in the ecosystem, a privacy management framework is desired. Before developing this framework, a collection of case studies involving multiple stakeholders must be analyzed to identify the different privacy requirements.

Plug-and-Play Service Composition: Application developers need a framework to create applications by composing various services quickly. If the developers are required to write hundreds of lines of code to compose different services, then the developers may have to carefully monitor and manage these interfaces or the gluing code which again introduce high management and maintenance overhead. Instead, the architecture should define a standard interface for the service providers, which can then be used to create a "plug-and-play" service composition framework. When the application developer composes an application by combining different services, the billing framework should create a single subscription or a bill for the application rather than forcing the developers to switch between multiple platforms to pay for various services.

Regulations and Standards: There is not a single owner in the multi-stakeholder deployment. Allowing a single stakeholder to define the standard and the policies may lead to a vendor lock-in problem since the leading organization may define protocols and APIs for applications with lack of interoperability. A governing body should, therefore, be formed to regulate the standards and usage policies. Such a governing body define the rules and must ensure that all the members in the ecosystem are treated fairly.

The implementation of the proposed framework is left to future work, but the readers are encouraged to read our prior work that presents a reference architecture for blockchain-based peer-to-peer IoT applications [26] and decentralized data marketplace [25] to understand how the blockchain technology can be used to address issues such as identity, trust, micropayments, among other things.

9 Conclusion

Majority of the IoT deployments in the past two decades have been deployed and managed by a single organization. Such implementations focused on meeting a single goal or an application. The single stakeholder deployment model leads to many real-world deployments with tens of IoT devices. In this vision paper, we have explained why the single stakeholder model could not result in a large-scale IoT application and motivated the need for a multi-stakeholder deployment model. Besides, we have presented real-world examples of ongoing multi-stakeholder efforts and show that the IoT deployments of the future are expected to rely on different stakeholders for services such as sensing, computation, and communication. Lastly, we have presented the open research questions and showed a reference architecture with a set of fundamental building blocks of multi-stakeholder IoT deployments to encourage the researchers and IoT enthusiasts to lead the development efforts towards the creation of multi-stakeholder large scale IoT applications. We believe that the large scale IoT deployments require the support of multiple stakeholders, including the community members, telecommunication operators, and hardware vendors.

Acknowledgements

This work is supported by the USC Viterbi Center for Cyber-Physical Systems and the Internet of Things (CCI).

References

[1] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, and J. C. Zhang, "What will 5G be?" *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, 2014.

[2] A. Banks and R. Gupta, "MQTT version 3.1. 1," *OASIS standard*, vol. 29, p. 89, 2014.

[3] S. Battle and B. Gaster, "LoRaWAN bristol," in *Proceedings of the 21st International Database Engineering & Applications Symposium*, ser. IDEAS 2017. New York, NY, USA: ACM, 2017, pp. 287–290.

[4] N. Blenn and F. A. Kuipers, "LoRaWAN in the wild: Measurements from the things network," *CoRR*, vol. abs/1706.03086, 2017.

[5] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and textInternet of Things: A survey," *Future Generation Computer Systems*, vol. 56, pp. 684 – 700, 2016.

[6] B. Clerckx, A. Lozano, S. Sesia, C. Van Rensburg, and C. B. Papadias, *3GPP LTE and LTE-Advanced*. Nature Publishing Group, 2009.

[7] B. P. Crow, I. Widjaja, J. G. Kim, and P. T. Sakai, "IEEE 802.11 wireless local area networks," *IEEE Communications Magazine*, vol. 35, no. 9, pp. 116–126, 1997.

[8] J. de Carvalho Silva, J. J. Rodrigues, A. M. Alberti, P. Solic, and A. L. Aquino, "LoRaWAN- a low power wan protocol for internet of things: A review and opportunities," in *2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*. IEEE , 2017, pp. 1–6.

[9] P. Dutta, D. E. Culler, and S. Shenker, "Procrastination might lead to a longer and more useful life." in *HotNets*. Citeseer, 2007.

[10] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645 – 1660, 2013.

[11] J. A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, and B. Heile, "IEEE 802.15. 4: A developing standard for low-power low-cost wireless personal area networks," *IEEE Metwork*, vol. 15, no. 5, pp. 12–19, 2001.

[12] S. Hasan, M. C. Barela, M. Johnson, E. Brewer, and K. Heimerl, "Scaling community cellular networks with communitycellularmanager," in *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*. Boston, MA: USENIX Association, 2019, pp. 735–750.

[13] G. T. Heineman and W. T. Councill, Eds., *Component-based Software Engineering: Putting the Pieces Together*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2001.

[14] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing—a key technology towards 5g," *ETSI*, vol. 11, no. 11, pp. 1–16, 2015.

[15] J. Im, S. Kim, and D. Kim, "IoT mashup as a service: Cloud-based mashup service for the internet of things," in *2013 IEEE International Conference on Services Computing*, June 2013, pp. 462–469.

[16] S. Kar, B. Chakravorty, S. Sinha, and M. P. Gupta, *Analysis of Stakeholders Within IoT Ecosystem*. Cham: Springer International Publishing, 2018, pp. 251–276.

[17] A. Keranen, M. Ersue, and C. Bormann, "Terminology for constrained-node networks," *Terminology*, 2014.

[18] B. Krishnamachari, J. Power, S. H. Kim, and C. Shahabi, "I3: an IoT marketplace for smart communities," in *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 2018, pp. 498–499.

[19] I. Lee and K. Lee, "The internet of things (IoT): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431 – 440, 2015.

[20] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless sensor networks for habitat monitoring," in *Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications*. ACM, 2002, pp. 88–97.

[21] B. A. Miller and C. Bisdikian, *Bluetooth revealed: the insider's guide to an open specification for global wireless communication*. Prentice Hall PTR, 2001.

[22] Nodle, "Connecting devices everywhere," 2019. [Online]. Available: https://nodle.io/

[23] C. Pham, "Communication performances of IEEE 802.15.4 wireless sensor motes for data-intensive applications: A comparison of waspmote, arduino mega, telosb, micaz and imote2 for image surveillance," *Journal of Network and Computer Applications*, vol. 46, pp. 48 – 59, 2014.

[24] R. Radhakrishnan and B. Krishnamachari, "Streaming data payment protocol (SDPP) for the internet of things," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018, pp. 1679–1684.

[25] G. S. Ramachandran, R. Radhakrishnan, and B. Krishnamachari, "Towards a decentralized data marketplace for smart cities," in *2018 IEEE International Smart Cities Conference (ISC2)*, Sep. 2018, pp. 1–8.

[26] G. S. Ramachandran and B. Krishnamachari, "A reference architecture for blockchain-based peer-to-peer IoT applications," *ArXiv*, vol. abs/1905.10643, 2019.

[27] G. S. Ramachandran, N. Matthys, W. Daniels, W. Joosen, and D. Hughes, "Building dynamic and dependable component-based internet-of-things applications with dawn," in *2016 19th International ACM SIGSOFT Symposium on Component-Based Software Engineering (CBSE)*. IEEE , 2016, pp. 97–106.

[28] J. Ren, H. Guo, C. Xu, and Y. Zhang, "Serving at the edge: A scalable IoT architecture based on transparent computing," *IEEE Network*, vol. 31, no. 5, pp. 96–105, 2017.

[29] A. Rotem-Gal-Oz, "Fallacies of distributed computing explained," 2006. [Online]. Available: http://www.rgoarchitects.com/Files/fallacies.pdf

[30] T. Saarikko, U. H. Westergren, and T. Blomquist, "The Internet of Things: Are you ready for what's coming?" *Business Horizons*, vol. 60, no. 5, pp. 667 – 676, 2017.

[31] A. Saeed, M. Faezipour, M. Nourani, and L. Tamil, "Plug-and-play sensor node for body area networks," in *2009 IEEE /NIH Life Science Systems and Applications Workshop*. IEEE , 2009, pp. 104–107.

[32] K. Samdanis, X. Costa-Perez, and V. Sciancalepore, "From network sharing to multi-tenancy: The 5G network slice broker," *IEEE Communications Magazine*, vol. 54, no. 7, pp. 32–39, 2016.

[33] L. Sanchez, L. Muñoz, J. A. Galache, P. Sotres, J. R. Santana, V. Gutierrez, R. Ramdhany, A. Gluhak, S. Krco, and E. Theodoridis, "Smartsantander: IoT experimentation over a smart city testbed," *Computer Networks*, vol. 61, pp. 217–238, 2014.

[34] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, 2017.

[35] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (coap)," Internet Engineering Task Force (IETF), Tech. Rep., 2014.

[36] Z. Sheng, C. Mahapatra, C. Zhu, and V. C. Leung, "Recent advances in industrial wireless sensor networks toward efficient management in IoT," *IEEE Access*, vol. 3, pp. 622–637, 2015.

[37] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[38] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," *Journal of Cleaner Production*, vol. 140, pp. 1454–1464, 2017.

[39] M. Turner, D. Budgen, and P. Brereton, "Turning software into a service," *Computer*, vol. 36, no. 10, pp. 38–44, 2003.

[40] T. Watteyne, J. Weiss, L. Doherty, and J. Simon, "Industrial IEEE 802. 15.4 e networks: Performance and trade-offs," in *2015 IEEE International Conference on Communications (ICC)*. IEEE , 2015, pp. 604–609.

[41] P. Wendell and M. J. Freedman, "Going viral: flash crowds in an open cdn," in *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement*. ACM, 2011, pp. 549–558.

[42] G. Werner-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J. Lees, and M. Welsh, "Deploying a wireless sensor network on an active volcano," *IEEE Internet Computing*, vol. 10, no. 2, pp. 18–25, 2006.

[43] F. Yang, N. Matthys, R. Bachiller, S. Michiels, W. Joosen, and D. Hughes, "μ PNP: Plug and play peripherals for the internet of things," in *Proceedings of the Tenth European Conference on Computer Systems*. ACM, 2015, p. 25.

[44] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014.

AUTHOR BIOGRAPHIES

Gowri Ramachandran is a postdoctoral researcher at the Center for Cyber Physical Systems and the Internet-of Things (CCI) at the University of Southern California. He received his Ph.D. from imec-DistriNet, KU Leuven, Belgium. His research interests include Internet-of-Things (IoT), smart cities, and blockchain.

Bhaskar Krishnamachari received his Ph.D. degree from Cornell University, Ithaca, NY, USA, in 2002. He is currently a Professor with the Department of Electrical and Computer Engineering, and Director of the Center for Cyber-Physical Systems and the Internet of Things. His research interests include the design and analysis of algorithms and protocols for the Internet of Things, Wireless Networks, and Distributed Systems.