The Internet of Things vs the Internet of Everything

David Lengel
Schreyer Honors College
Penn State Behrend
Erie, PA
dal5441@psu.edu

***Abstract*—The purpose of this paper is to establish the similarities and differences between the Internet of Things (IoT) and the Internet of Everything (IoE). With the recent developments in the IoE, and with the IoT still being relatively new, the similarities and differences between the two platforms is not clearly defined. In order to make this more clear, this paper looks into the architectures, platforms, and technologies of both the IoT and IoE by providing definitions, background information, and real-world examples for each. By doing this, the paper draws clear similarities and differences between the two platforms and provides the reader with concise conclusions from each topic.**

***Index Terms*—Internet of Things, Internet of Everything**

I. Introduction

A. The Internet of Things (IoT)

The Internet of Things (IoT) can take on many different meanings depending on its scope and application, be it manufacturing, logistics, product development, or a number of other areas [13]. In the past, the term "Internet of Things" was "proposed to refer to uniquely identifiable interoperable connected objects with radio-frequency identification" [27]. This definition is somewhat vague and specific to certain scenarios. In today's world, and specifically within the scope of computer networking, the internet of things can be defined more simply and definitively.

To define the IoT, *things* or *objects* must first be given meaning. Things or objects, are physical devices, such as "Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile phones, etc" [10]. Using this definition, the IoT can be defined as a variety of these things interacting with each other to reach common goals [10].

In a larger sense, the IoT refers to creating connections from these sensors in the world to computers that make sense of incoming data and present it to people, and then allowing people to send instructions back to devices. The goal of this is to lead to a "highly distributed network of devices communicating with human beings as well as other devices" in order to open opportunities for larger numbers of practical applications that "promise to improve the quality of. . .lives" [26]. This paper will take a deeper look into the IoT, specifically in three areas: its architecture, platforms, and technologies.

As the IoT has been developed and improved over the years, multiple architectures have been proposed and/or put into place. Most of these architectures divide the internet of things into different layers, and these architectures differ in how the layers are divided and the function of each layer in the IoT. Although architectures may vary, many are similar because they fall under one of two categories: Service-Oriented Architectures (SOA) or cloud-based architectures. Many SOAs have been proposed, but one of the most prevalent is a four-layer architecture with Sensing, Networking, Service, and Interface layers [27]. Another IoT architecture has been proposed and is based on the cloud [15]. Both of these architectures will be discussed in more detail later in this paper.

With the developing architectures and possibilities of the IoT also comes many competing platforms attempting to support it. While in many markets, such as for gaming consoles and operating systems, there are only a few major competitors that have withstood the test of time, this is not yet so with the IoT. It is still relatively new and being developed, and there are a large number of companies creating their own platforms to incorporate and build on the IoT. These companies are developing different types of platforms for the IoT, enabling the use of the IoT in new and varying ways. Different types of platforms being developed include Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS).

As a result of more companies developing IoT platforms, the technologies associated with the IoT are growing and becoming more advanced. Some areas in which IoT technologies are being developed include identification, sensing, communication, hardware and software computation, and semantics [9]. Advances in these technologies make IoT applications possible in a number of industry domains.

B. The Internet of Everything (IoE)

It is believed that the Internet of Things will naturally evolve, "due to recent advancements in big data, connection technologies, and smart devices" [28], into the Internet of Everything (IoE). The IoE is the linking of network sensors and devices to and from each other through the internet "in networks of billions or even trillions of connections" [12]. These devices have the ability to send data and automatically receive instructions for operations without explicit human interaction. Such an environment has the potential for automation of processes, higher levels of data collection, and faster communication, making it very desirable to be researched and developed to evolve from the IoT.

According to Snyder and Byrd, “the key to this evolution is the maturing fields of AI, cognitive computing, and machine learning” [22]. This evolution will likely be taking place much more rapidly in the near future. A recent study by Cisco predicts that the “IoE is projected to create $14 trillion net-profit value . . . from 2013 to 2022” [8]. In addition to this study, “IDC projects that by 2020, there will be 212 billion ‘things’ in the world” [12]. With such a projected growth in the IoE, so too will come a growth in its architecture, platforms, and technologies, each of which will be discussed in this paper.

As the IoE has yet to be put into place on a large scale, many architectures have been proposed. Among these architectures, two prevailing patterns can be found. The first divides the IoE into layers, focusing more on the types of devices and functions of software to divide the IoE into layers. In general, this architecture breaks the IoE into seven layers: Device, Object, Client, Propagator, Filter Gateway, Integrator, and Application [14]. The second architecture is more focused on using the cloud and its applications in the IoE to divide it into layers. Such an architecture is generally divided into four layers: Fog, Stratus, Alto-cumulus, and Cirrus [8]. While the names of these layers may not have much meaning at this point in the paper, they will be discussed later in detail.

With the projected growth of the IoE in the present and near future, many companies are developing competing IoE platforms. For the most part, these platforms focus on the cloud in order to take the things from the IoT and add to their numbers and connect them all to each other. At present, many companies, new and old, are developing platforms for the IoE . The cloud-based platforms that are being created by these can be divided into three main categories: Sensing and Actuating Infrastructure as a Service (SAIaaS), Sensing and Actuating Platform as a Service (SAPaaS), and Sensing Data and Analytics as a Service (SDAaaS) [8].

Through the cloud-based platforms made possible by the IoE, new technologies can be created to provide a wide variety of IoE applications. Some of these technologies are in the areas of remote tracking and monitoring, real-time resource optimization and control, and smart troubleshooting (identifying, diagnosing, and repairing issues) [8]. These different technologies can be applied to a large variety of industry domains that will be discussed in further detail.

II. Architectures

A. IoT Architectures

1) Service-Oriented:

According to [27], many architectures have been propsed for the IoT, most varying from three to five layers. Despite the number of different proposed architectures, two of the most prevalent architectures for the IoT are service oriented and cloud-based architectures. Service oriented architectures (SOA) typically consist of four layers: Sensing, Networking, Service, and Interface [27]. Keeping in mind that in the IoT, data typically flows only from devices up to a user interface, the Sensing layer is closest to the physical devices and the Interface layer is closest to the user interface. A model of this can be seen in Figure 1.

The sensing layer includes the *things* of the IoT, which are the devices that either sense environmental conditions or control the environment. For sensing devices, this layer provides for sensed environmental conditions to be converted to data. For controlling devices, this layer provides for devices to be able to act on instructions. It is important to note that in a single process, devices may not send data and receive instructions. These must be done in separate processes, as the IoT does not support automation.

The networking layer is the next layer going up the architecture. This layer connects devices for two major purposes. First, devices are connected to the layers above them. Without this functionality, devices would not be able to send or recieve data from other layers, blocking the flow of information necessary for the IoT. Second, devices are interconnected with each other so that information can be shared between them. This is important because it gives relevance to devices that are be closely related, allowing for more in-depth and meaningful data to be sent. This is important for the upper two layers that evaluate and manage data and devices.

The service layer is next. This layer ”creates and manages services . . . to satisfy user needs” [27]. The service layer includes four components. First is service discovery, identifying available objects that can offer information and services. Second is service composition, identifying desired services and then scheduling or re-creating the most suitable services possible to meet the request. Third is trustworthiness management, creating a trustworthy system that can evaluate and use provided information. Fourth is service APIs, supporting interactions between services [27]. All of these components working together allow the service layer to provide necessary, trustworthy, interactive services to the IoT platform.

The final layer is the interface layer. This layer provides for the application and user interaction with the IoT [27]. This layer presents information sent up through the architecture by sensing devices in meaningful way through an application. This allows a user to view and make sense of that information. This layer also allows a user to provide information which can be converted to instructions and sent down the architecture to controlling devices.

2) Cloud-Based:

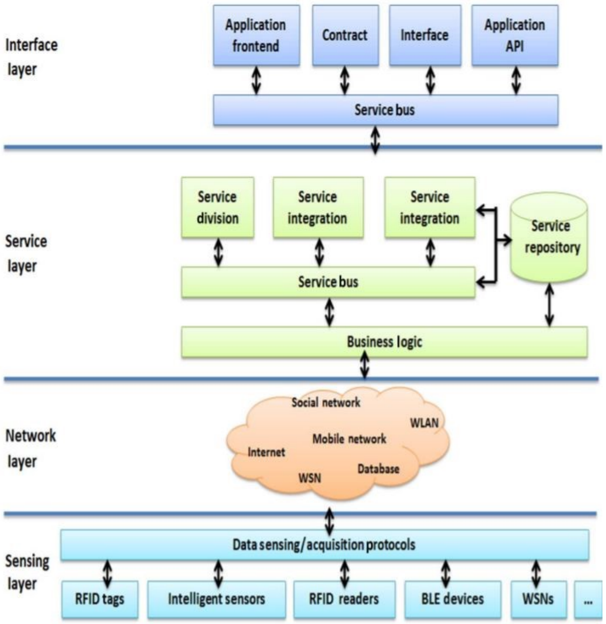
As previously stated, another architecture for the IoT is a cloud-based architecture. This architecture has three main components: Virtual Resource Pool, IoT Infrastructure, and IoT Cloud. For the architecture being studied in this paper, the IoT Cloud uses the Virtual Resource Pool and is above the IoT Infrastructure. In case this is not clear, a model of this architecture can be seen in Figure 2.

The first layer that will be looked into is the IoT Infrastructure. This layer ”consists of all IoT devices and the supporting access networks” [15]. Similar to the sensing and network layers of the previous architecture, this layer has all of the physical devices of the IoT platform, and also handles the sending of data from and instructions to these devices.

The next layer is the IoT Cloud. Within the IoT Cloud are databases to store data, reverse proxy to handle the number of physical devices in the system, and load balancing to evenly distribute computing power. Also in the IoT Cloud are the Application Servers, which are ”often considered to be the most important component of the IoT cloud since they are resopnsible for offering business services to customers” [15]. Like the Interface layer of the previous architecture, this part of the IoT cloud provides the facilites and environment to run applications based on certain protocols. These protocols operate via a ”topic-based publish-subscribe model” [15]. This means that all clients subscribed to a topic can receive a message when a client publishes that message to the topic.

The final component is the Virtual Resource Pool. While not technically a part of the cloud layer, this component provides computational power to the cloud layer. This is possible because of virtualization, wherein IoT cloud services can be deployed on virtual machines (VMs) which run on physical machines. According to [15], ”by employing the virtualization technique, a virtual resource pool can be established on several physical mahcines that contain all the hardware resources and can assign them to different VMs on demand”. This means that servers in the IoT Cloud layer can be provided with appropriate resources to meet their individual demands by the virtual resource pool.

Fig. 1. IoT Four-Layer Service-Oriented Architecture [27]

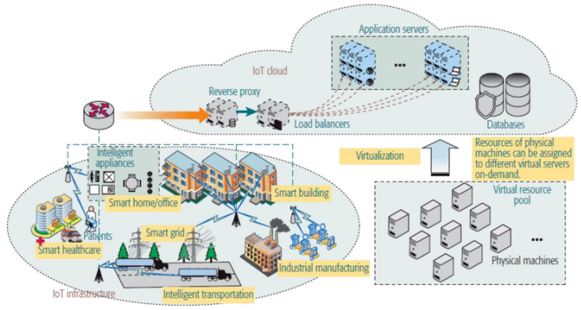


B. IoE Architectures

1) Function-Focused:

The first IoE architecture that will be discussed divides the IoE into layers depending on the types of devices and functions of software throughout the IoE. There are seven layers in this architecture: Device, Object, Client, Propagator, Filter Gateway, Integrator, and Application [14]. The device layer is closest to the physical devices, while the application layer, as the name implies, is closest to the applications that take advantage of the IoE and can see the ”big picture”. A simple model of these layers can be seen in Figure 3.

Fig. 2. IoT Cloud-Based Architecture [15]



The device layer is the first layer is similar to the IoT sensor layer. This layer contains the physical devices themselves, be they sensors that collect environmental data or controllers that act on the environment.

The second layer is the object layer. An object is a board or housing that contains one or more devices packages together.

The third layer is the client layer. At this layer, a software-enabled client ”manages the collection of data from and distribution of messages to the objects” [14]. The client software may either run on a smart device or ”general-purpose PC, laptop, tablet, or mobile phone” [14].

Fourth is the propagator level, which is a node or server that connects the device and object clients to the internet. This level exists in the locality of physical devices, and are likely software applications running on standard hardware.

The fifth level is the filter gateway level, which exists in the same node or server as the part of the Propagator level from which it receives data. As the name suggests, this layer ”filters” data coming from clients so that meaningful and significant data is sent to the next level.

The sixth level, the integrator level, ”brings together the data from multiple sources” [14] and combines that data in order to transform it and derive patterns from it. The integrator level software ”is likely to run in a data-centre environment” [14].

Finally, the seventh level, the application level, is ”where the full value and capabilities of the IoE . . . are exploited”. This may comprise large systems running in data centers, or even mobile or web applications that access data through web servers [14].

2) Cloud-Based:

The second IoE architecture that will be discussed here focuses on the application of the cloud with the IoE, and divides it into layers based on how the cloud can be used throughout the IoE. With this architecture, there are four layers. Conveniently, the names of these layers are clouds: Fog, Stratus, Alto-cumulus, and Cirrus. Fog clouds are the lowest and Cirrus clouds are among the highest in Earth’s atmostphere, and the layers of this IoE architecture can be thought of in a similar way. The fog layer is closest to devices, while the cirrus layer is the highest-level cloud environment [8]. A model of this can be seen in Figure 4.

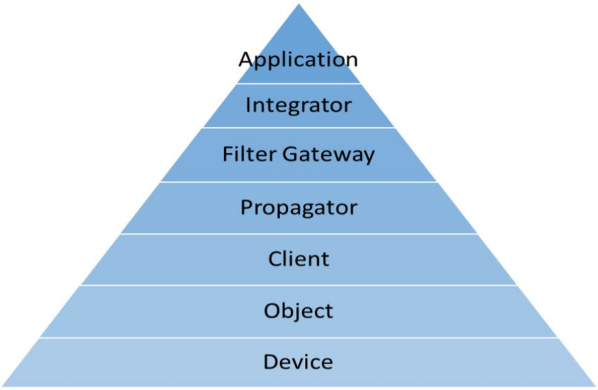
Similar to the IoT sensor layer and the first IoE architecture's device layer, the fog layer includes all physical devices and objects that collect environmental data and control the environment based on received instructions.

The stratus layer ”consists of thousands of clouds whose main resources are sensory devices” [8]. Each stratus-layer cloud manages different groups of devices that share similar ”features, contexts, or priorities” [8]. In short, the stratus layer acts as an interface between the fog layer and the alto-cumulus layer by abstracting groups of data from the physical world and presenting it to the alto-cumulus layer.

The alto-cumulus layer also acts as an interface, but between the stratus and cirrus layers. The alto-cumuls layer translates policy, enables transactions, facilitates negotiations, and coordinates interactions between these two layers so that information can be sent back and forth efficiently and without violation of terms [8].

The final layer, the cirrus layer, is the highest layer in the cloud-based IoE architecture. Its main role is to interact with customers and satisfy their requests by communicating back down to lower layers. This top layer depends on all layers because it connects devices (fog), manages device virtualization and embedding (stratus), manages cloud domains (alto-cumulus), and abstracts cloud services to customers (cirrus) [8].

Fig. 3. IoE Seven-Layer Function-Focused Architecture [14]

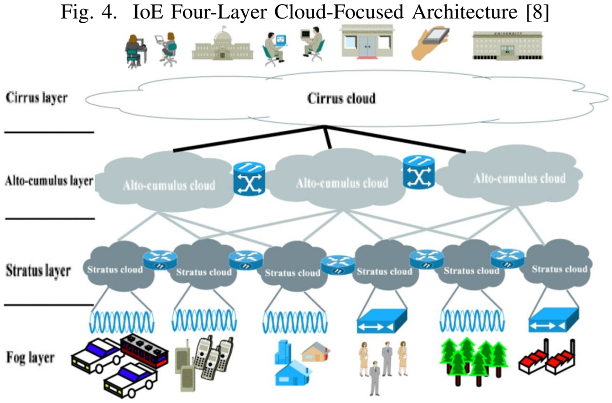


C. IoT Architecture vs IoE Architecture

1) Similarities:

In many ways, the IoT and IoE architectures are very similar. These similarites stem from the very definition of the IoE, which states that it is an evolution of the IoT. While its scope and applications may be different, the architecture on which it is based is complementary to that of the IoT. Take, for example, the given five-layer IoT architecture and the first, seven-layer IoE architecture provided in the previous sections. Both of these architectures are very similar in the purposes, components, and relative locations of each layer.

Fig. 4. IoE Four-Layer Cloud-Focused Architecture [8]



First, the lowest layers are responsible for sensing and controlling the environment through the devices located in them. The layer that does this in the IoT is the Sensing layer, and in the IoE are the Device and Object layers.

Going up the architecture, the next layers are those that connect the devices with the upper layers. For the IoT, this is done in the network layer, and for the IoE, the client and propagator levels. The purpose of the IoT network layer is to send data from the sensing layer devices to the service layer services and vice versa. Similarly, the client and propagator levels work together in the IoE to send data between the devices and the filter gateway layer.

Moving on, the next layers have the purpose of receiving data from the network and presenting it to the application/interface. The IoT service layer does this by finding and implementing different services to refine and present data to the application layer. The IoE filter gateway layer and integrator level serve the same purpose by filtering data, bringing it together from multiple sources, and deriving patterns from it.

Finally, the top layers are to present data that has been passed up through the layers to top-level user of the platform. In the case of the IoT's application level, this top-level user is an actual person who views the data presented to the them and then makes a decision based on that data. With the IoE, this top-level user is typically a large system or a mobile/web application that will make a decision based on the data it is presented. In either case, a top-level user views that data and makes a decision.

Along with similarities in functions, some of these layers also have similarities in their physical locations. The IoT Sensing layer and the IoE Device, Object, and Client layers are all located within the physical devices of each platform. The IoT Service layer and the IoE Propagator, Filter Gateway, and Integrator layers are all located in centralized servers. The IoE Integrator level servers may be different from the Filter Gateway and Propagator level servers as the Integrator level is typically associated with data centers, but they are all still servers directly between the devices and the application/interface. Finally, the IoT Interface layer and the IoE Application layer are both used for customer and/or system interface, and so they are typically in applications, web services, and data centers. While there are many similarities between these two device-based architectures, they are not the only architectures with similarities between the IoT and IoE.

The two cloud-based architectures can also be compared for their similarities. Both architectures' lowest levels contain the physical devices of the platform. In the IoT this is part of the IoT Infrastructure, while in the IoE it is the Fog Layer. The next level up in each architecture manages the data going to and from these devices and connects it to the upper layers of the architecture. This is still under the IoT Infrastructure component, but part of the IoE Stratus layer. Finally, the two cloud-based architectures are similar in their top layers. Part of the IoT cloud layer is the Application servers which provide the top-level cloud services of the platform to the customers. This is also the responsibility of the IoE Cirrus Layer. While it may reasonably be speculated from these claims that the IoT and IoE share mostly similarities in architectures, it is crucial to note thier differences.

2) Differences:

One difference between the IoT and IoE architectures can be seen when comparing the IoT Service-Oriented (Fig. 1) and IoE Device-and-Software-Focused (Fig. 3) architectures' number of layers. In this case, the IoE contains three more layers than the IoT because more layers are added to the IoE to deal with collection, grouping, and refinement of data. It is necessary that the IoE have more discrete layers for this process because the IoE will have more devices and data than the IoT.

Another difference can be seen when comparing each platform's cloud-based architecture. The IoE has the Alto-cumulus layer responsible for translating policy, enabling transactions, facilitating negotiations, and coordinating interactions between the layers above and below it, with no such equivalent in the IoT cloud-based architecture. As with the previous difference, this could be due to the greater size and complexity of the IoE compared to the IoT. A distinct layer for such actions makes sense in the IoE, because it has a greater variety of different devices and clients that it is responsible for coordinating.

III. Platforms

A. IoT Platforms

An analysis of current IoT platforms by [19] identified and surveyed 39 IoT platforms currently on the market. According to [19], the list of almost 40 platforms is not an exhaustive one, but rather a "representative sample" of the available platforms. Most platforms can be identified as one of these types: Platform as a Service (PaaS), Software as a Service (SaaS), or Infrastructure as a Service (IaaS).

1) Different Types of Platforms:

With PaaS, the provider of the platform makes most choices in how the application infrastructure operates. "PaaS typically provides a complete set of tools and technology, from the interface design, to process logic, to persistence, to integration". These choices can include, but are not limited to, type of Operating System used, APIs, programming language, and management capabilities. PaaS works by providing users with access to the providers' servers, from which users can develop applications. In this way, PaaS is useful at hiding the complexity between a client and virtual server, and can increase developers' productivity and organization. [16] Such a platform can be utilized in the IoT by providing cloud computing services for IoT devices, data, applications, and users. More services for the IoT that were not already mentioned can include storage facilites, device management, device connectivity, backup mechanisms, and online support. [19]

SaaS refers to the combining of data using cloud computing capabilities [19]. SaaS "offers users the hardware infrastructure, the software product and interrelates with the users through a portal." In other words, with SaaS there is a common code and common data that the vendor provides to customers to use. Because of this, the application and infrastructure are shared across all customers, each clients' customization options are constrained, and the vendor has control over future revisions and development of the software [11]. Providers of platforms that use SaaS in the IoT typically install and operate this software in the cloud, authorizing and enabling an application for IoT use in the cloud [23].

Finally, developers can offer the IoT IaaS, providing third-party application developers with access to an IoT infrastructure that they can use to work with the IoT without having to manage an infrastructure themselves [17]. Such a service includes a combination of "hosting, hardware provisioning, and basic services needed to run a cloud" [18] infrastructure in the IoT. More specifically, according to [18], IaaS provides for the following uses: "access to shared resources on need basis", "details like server images on demand, storage, queuing, and information" about available resources, and "full control of server infrastructure", all without disclosing details like location and hardware to clients.

2) Examples of Platforms:

There are a number of PaaS IoT platforms that support this claim, and listed are only a select few of those. The platform developed by Carriots is a PaaS where "data is stored on the platform and access keys are required to access it". Another is a platform developed by ThingSpeak, which "provides a server that may be used to store and retrieve IoT data" and provides "visualization tools" and "enables the creation of widgets" so that users can easily visualize this data. A third is developed by Xively. Very similar to the others, data is stored on Xively's servers, and Xively provides API's to users. There are many more examples, but they are all very similar to these three PaaS platforms. [19]

As with PaaS, there are many SaaS platforms being developed for the IoT that confirm SaaS platforms' use in the IoT. A SaaS platform by IFTTT ("if this then that") allows users to use the software directly to create services to automate various Internet tasks. These services have the option of being personal or shared, and this is up to the discretion of the user because of the SaaS platform. Another platform is developed by SkySpark, which is a platform that can be "locally installed on a private server or on a cloud" and "enables analytic tools for big data processing".

There are a number of available platforms that could provide an infrastructure upon which to build the IoT. One such company offering an IaaS for the IoT is the company Trilliant. Trilliant is an "energy industry communication platform" working on a "smart grid" for electrical systems, where devices can monitor and provide information about power grids to people who can use that information to make changes in the grid and improve efficiency and energy usage. Trilliant offers electrical companies the "hardware, software, and services" that make the smart grid possible. [**?**]. Another IaaS platform is being offered by NEC. NEC provides a "broad range of IT products and services through software, hardware, integration, and consulting". NEC is now looking to integrate their infrastructure with the IoT for social infrastructure and corporate use. [**?**]

B. IoE Platforms

At the time this paper is being written, companies are developing platforms for the IoE. While two major companies, Cisco [7] and Qualcomm & At&T [6], may be the most recognizable companies working on IoE platforms, there are still a number of smaller companies making progress in this area as well. According to [8], there are three main, cloud-based models being developed for IoE platforms.

1) Different Types of Platforms:
The first platform model is Sensing and Actuating Infrastructure as a Service (SAIaaS). In this model, phsycial sensor resources and sensor and actuator network (SAN) resources "serve multiple sensing tasks concurrently" [8]. Users have allocated virtual instances of resources over which they have full control, but they cannot make changes to physical resources (i.e., SANS and sensors). [8]

The second platform model is Sensing and Actuating Platform as a Service (SAPaaS). This model provides users with APIs and libraries that they can use develop their own applications, without changing the physical SANs. Users still have full control over their applications and resources, but cannot alter the physical or virtual infrastructure. [8]

The third platform model is Sensing Data and Analytics as a Service (SDAaaS). In this model, users are "only interested in the context in which sensed data is collected, its accuracy, and its sufficiency to be able to generate meaningful inferences" [8]. Users of this model do not have control over how or where data is collected or the setup of sensors and software. They are only concerned with the data and its availability and accuracy. [8]

2) Examples of Platforms:
According to [8], Numerex is a company that utilizes SAIaaS. Numerex is a provider of machine to machine (M2M) products and technology. The company provides pre-configured, cloud-based technology and services to customers on a subscription basis. These customers can use Numerex's pre-existing infrastructure to monitor and alter their IoE platform. [3]

Two companies that use SAPaaS are Ubidots and Axeda [8]. Ubidots provides its customers with APIs to connect "hardware and digital inputs to Ubidots Cloud where it can be analyzed" [5]. Axeda provides access to its "data integration and application development platform" which allows customers to manage connected IoE products [2].

Finally, two companies that use SDAaaS are Arkessa and Paraimpu. Arkssa provides deployable software to its customers that allows devices to be connected with each other in a M2M network, enabling the IoE [1]. Similarly, Paraimpu deploys software to connect physical devices, APIs, and services to the web so that they can communicate with each other and form an IoE environemnt [4].

C. IoT Platforms vs IoE Platforms

1) Similarities:
The IoT and IoE have many similarities in the types of platforms available for each.

The IoT and IoE are similar in some of their cloud-based models. First, the IoT's PaaS model is similar to the IoE's SAPaaS model. These models give customers access to a company's platform as a service. They provide users with the tools to allow them to host and execute their own virtual applications without altering the phsyical or virtual infrastructure.

Also, the IoT's SaaS model is similar to the IoE's SDAaaS model. These models deploy software to customers which allows them to develop applications using their own hardware. They allow users to combine data and make inferences from it without having to know the details about sensors or the software running on them.

In addition, there are similarities between the IoT IaaS and the IoE SAIaaS. Both give customers access to virtual instances of resources that they can control and use to develop applications, while not revealing the physical resources.

As the IoT is naturally evolving to become the IoE, many companies devloping platforms for the IoT are also now working on creating IoE platforms.

When comparing two separate studies by [19] and [8], eight of such companies can be identified. However, this is only a small fraction of such cases, as each of these references only reviews a small, representative sample of companies in each market.

2) Differences:
While they may not be as numerous or distinct, there exist some differences between IoT and IoE platforms. These differences are mainly present in the companies that are developing these platforms.

Many companies are developing for both the IoT and IoE, but there are still some companies that have been and continue developing for purely the IoT as well as other newer companies that are developing only for the IoE.

IV. Technologies

A. IoT Technologies

1) Technology Fields:
Some of the most promenant IoT technologies in use can be grouped into one or more of these fields: identification,

sensing, communication, hardware and software computation, and semantics [9].

One of the most crucial parts of identifying technology is the ability to efficiently and uniquely address each object and its address. Objects working together for identifying in an IoT network need to be unique because ”addressing assists to uniquely identify objects” [9]. This allows for more than just unique environmental factors to monitored, but also for them to be monitored uniquely across space and time.

Sensing technologies collect and store data from objects within the IoT network. The technologies in this field can include devices such as ”smart sensors, actuators or wearable sensing devices”. Some companies also offer ”smart hubs” and mobile applications that allow customers to ”monitor and control thousands of smart devices and appliances inside buildings”. Single Board Computers are often used with the technologies to connect them to a ”central management portal” to provice data to the customers.

Communication technologies connect objects together to deliver ”specific smart services”. Devices in this field include RFID readers, Near Field Communication, ultra-wide bandwidth, and other similar devices with the ability to connect and communicate. Other devices in this field do not necessary need to communicate directly, but can also utilize communication links such as WiFi, bluetooth, or LTE.

Computational technologies are typically not devices in the lower sensing layer, but are heigher up in the service and interface layers. They are processing units and software applications that represent the ”computational ability” of the IoT. Along with the typical hardware and software platforms, cloud platforms have also been utilized as a computational part of the IoT lately, specifically for the possiblities it offers with the collection and computation of big data.

Technologies in the semantics fields are similar to computational technologies, but instead of operating on data, they determine the correct services to meet demands and send data to those services.

2) Industry Domains:

As previously discussed in this paper, the IoT has been revolutionary in its ability to connect a large number of devices and many companies have been working to develop IoT platforms and technologies. This has been and is leading to a diverse range of industry domains of which the IoT is a major component. According to [21], some of these domains are smart homes, smart farms, smart grids, and smart cities.

Smart home refers to the IoT in home control. This can include, but is not limited to, contolling appliances, thermostat, windows shades, and lights [24].

Smart farming is using IoT devices to get more precise information on crops in order to improve crop yield and ”reduce production costs by removing the use of non-essential pesticides or fertilizers” [20].

Smart grids use the IoT to collect data on energy of large-scale operations and use that data to help users manage energy consumption and usage of large-scale operations [25].

Lastly, the concept of smart cities aim to integrate IoT communication with social and online network infrastructures to aid in urbanization, energy consumption, and big data collection and computing to aid in population growth, energy efficiency, urbanization, and economy.

B. IoE Technologies

1) Technology Fields:

As with IoT technologies, IoE technologies can be categorized into several fields. For the IoE, these groups are remote tracking and monitoring, real-time resource optimization and control, and smart troubleshooting [8].

Devices that remotely track and monitor ”things of interest in real time” [8] allow for environmental factors to be sensed and stored, as well as alerts to be raised and actions to be taken based on those factors.

Devices that can be grouped into the real-time resource opimization and control category enable optimization and control of resources that vary from one application domain to another. Devices in this category use the information gathered from environmental factors and control the environment based on those factors.

Lastly, devices in the smart troubleshooting group identify, diagnose, and repair remote problems. These devices may present users with useful information to resolve problems when they arise, perform preventative diagnostics and automated maintenance on equipment, automate network troubleshooting, and detect and locate defects in systems.

2) Industry Domains:

Due to the possibility of more devices and automation made available by the IoE, as well as a growing number of companies developing IoE platforms, the IoE is being integrated into more and more industry domains. Along with IoT fields like smart homes, smart farms, smart grids, and smart cities, there are many examples of domains that can be found within the fields of technology discussed in the previous section.

Remote tracking and monitoring can include the tracking and monitoring of animal behaviors, environmental conditions, agriculture, survellance and security, healthcare, smart meters, and aviation and aerospace safety.

Real-time resource optimization and control can be applied to waste management, smart parking, traffic control, and healthcare.

Smart troubleshooting applies to the identifying, diagnosing, and repairing of issues and inefficiencies in aviation and aerospace, automotive, network systems, buildings, smart grids, and oil and gas pipeline fields.

C. IoT Technologies vs IoE Technologies

1) Similarities:

Similarities between IoT and IoE technologies exist in certain technology fields and in certain industry domains.

The first technology fields where similarities exist is in the IoT field of sensing and the IoE field of monitoring. Each of these fields deals with the sensing of environmental factors by devices in the IoT sensing and IoE device layers.

The next technology fields with similarities are the IoT identifying field and IoE montioring fields. These fields deal with the unique identification and tracking of object in the environment.

There are also similarities between some IoT and IoE industry domains.

As previously discussed in the paper, the IoE is the natural evolution from the IoT. As such, the domains where IoT platforms and technologies are being developed are also seeing a growth in IoE platforms and technologies.

2) Differences:
While there are a number of similarities, there are also some differences between IoT and IoE technologies. For the most part, these differences stem from the greater possibilities made available by the IoE, such as a larger number of connected devices and the capability of bidirectional communication in a single process without human intervention.

The first of these differences is the IoE technology field of real-time optimization and control. This field deals with the automated process of collecting data and controlling the environment, without human intervention. This is an example of the bidirectional communication made possible by the IoE, but is not a part of the IoT.

Another difference in technology fields is the IoE smart troubleshooting field. Similar to real-time optimization and control, the smart troubleshooting process does not require human interaction. It collects data from a system, then diagnoses and repairs the problem.

V. Conclusion

In the introduction to this paper, the two main differences between the IoT and IoE were defined as the IoE's much larger number of connected devices, and the IoE's ablity to both receive data from and send instructions to devices without human interaction. These two differences were used to set the IoT and IoE apart for the purposes of this paper, allowing similarities and differences to be drawn in the areas of architectures, platforms, and technologies.

A. IoT and IoE Similarities

1) Architectures:
The architectural similarities between the IoT and IoE stem from the IoE being an evolution of the IoT, and can clearly be seen in comparing architectural layer functions and locations between the IoT and IoE. In the paper, a service-oriented and cloud-focused architecture was provided for each platform. Between the two service-oriented architectures and the two cloud-focused architectures, most layers from top to bottom have similar functions in the sending, receiving, and operation of data, as well as in the physical locations of such layers in the network.

2) Platforms:
The similarities between the IoT and IoE are mostly in the types of platforms available for each. While they may be referred to by different names, the different types of functionality and deployment platforms the IoT match those of the IoE.

Also, many companies who began to develop IoT platforms are also developing platforms for the IoE. Most of these companies continue to develop the same types of platforms for the IoE as they do for the IoT.

3) Technologies:
Many similarities between IoT and IoE technologies can be found in certain technology fields. These are in key fields that the IoT was designed for, and were continued into the IoE because they are crucial for many processes of such platforms.

There are also many similarities to be found in the industry domains of each. As with the similarities in technology fields, the domains where IoT platforms and technologies are being developed are also seeing a growth in IoE platforms and technologies.

B. IoT and IoE Differences

1) Architectures:
The architectural differences between the IoT and IoE are not as numerous as the similarites. These differences are mostly apparent in the higher number of layers and cloud-based functionality of the IoE. This can attributed to the higher complexity of the IoE, requiring more layers and functionality to operate when compared to its IoT counterpart.

2) Platforms:
Similar to the architectures, the differences between IoT and IoE platforms are outweighed by the similarities. The main difference between the two is in the companies that develop either purely for the IoT or for the IoE, but not both.

3) Technologies:
Setting it apart from the other differences, the differences between IoT and IoE technologies are about as numerous as the similarities, and growing. These differences mostly stem from the greater possiblities made available by the IoE. The IoE can support more varied and technologically demanding fields, allowing for more technological possbilities than the IoT.

References

[1] Arkessa. https://www.iotone.com/supplier/arkessa/v55.

[2] Axeda machine cloud. https://www.iotone.com/software/axeda-machine-cloud/s378.

[3] Numerex. https://www.iotone.com/supplier/numerex/v673.

[4] Paraimpu. https://www.iotone.com/supplier/paraimpu/v680.

[5] Ubidots iot application development platform. https://www.iotone.com/software/ubidots-cloud/s71.

[6] Qualcomm and at&t develop internet of everything development platform. *Internet Business News*, Jan 08 2013. Copyright - (Copyright M2 Communications, 2013; Last updated - 2013-01-08.

[7] Chris white - svp, internet of things and internet of everything, global sales, cisco systems, inc, Jun 05 2016.

[8] Sherif Abdelwahab, Bechir Hamdaoui, Mohsen Guizani, and Ammar Rayes. Enabling smart cloud services through remote sensing: An internet of everything enabler. *IEEE Internet of Things Journal*, 1(3):276–288, Jun 2014.

[9] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials*, 17(4):2347–2376, Fourthquarter 2015.

[10] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer Networks*, 54(15):2787–2805, Oct 2010.

[11] Alexander Benlian and Thomas Hess. Opportunities and risks of software-as-a-service: Findings from a survey of it executives. *Decision Support Systems*, 52(1):232–246, July 2011.

[12] Ruthbea Yesner Clarke. Smart cities and the internet of everything: The foundation for delivering next-generation citizen services. *Alexandria, VA, Tech. Rep*, October 2013.

[13] Jim Euchner. The internet of things. *Research-Technology Management*, 61(5):10–11, Sep 2018.

[14] Paul Gerrard. Internet of everything - architecture and risks, Jun 2014.

[15] L. Hou, S. Zhao, X. Xiong, K. Zheng, P. Chatzimisios, M. S. Hossain, and W. Xiang. Internet of things cloud: Architecture and implementation. *IEEE Communications Magazine*, 54(12):32–39, December 2016.

[16] George Lawton. Developing software online with platform-as-a-service technology. *Computer*, 41(6):13–15, June 2008.

[17] Fei Li, Michael Voegler, Sanjn Sehic, Soheil Qanbari, Stefan Nastic, Hong-Linh Truong, and Schahram Dustdar. Web-scale service delivery for smart cities. *IEEE Internet Computing*, 17(4):78–83, July 2013.

[18] Sunilkumar Manvi and Gopal Shyam. Resource management for infrastructure as a service (iaas) in cloud computing: A survey. *Journal of Network and Computer Applications*, 41:424–440, May 2014.

[19] Julien Mineraud, Oleksiy Mazhelis, Xiang Su, and Sasu Tarkoma. A gap analysis of internet-of-things platforms. *CoRR*, abs/1502.01181, 2015.

[20] Aekyeung Moon, Jaeyoung Kim, Jialing Zhang, and Seung Woo Son. Evaluating fidelity of lossy compression on spatiotemporal data from an iot enabled smart farm. *Computers and Electronics in Agriculture*, 154:304–313, November 2018.

[21] Mostakim F. Sheik Mohammad, Nak-Myoung Sung, Il-Yeup Ahn, Minwoo Ryu, and Jaeseok Yun. Building iot services for aging in place using standard-based iot platforms and heterogeneous iot products. *Sensors*, 17(10):2311, 2017.

[22] Tom Snyder and Greg Byrd. The internet of everything. *Computer*, 50(6):8–9, Jun 2017.

[23] Antonio Solano, Raquel Dormido, Natividad Duro, and Miguel S. Juan. A self-provisioning mechanism in openstack for iot devices. *Sensors*, 16(8):1306, 2016.

[24] Biljana L. Risteska Stojkoska and Kire V. Trivodaliev. A review of internet of things for smart home: Challenges and solutions. *Journal of Cleaner Production*, 140:1454–1464, 2017 2017.

[25] Sanjana Kadaba Viswanath, Chau Yuen, Wayes Tushar, Wen-Tai Li, Chao-Kai Wen, Kun Ju, Cheng Chen, and Xiang Liu. System design of the internet of things for residential smart grid. *IEEE Wireless Communications*, 23(5):90–98, October 2016.

[26] Feng Xia, Laurence T Yang, Lizhe Wang, and Alexey Vinel. Internet of things. *International Journal of Communication Systems*, 25(9):1101—-1102, Sep 2012.

[27] Li Da Xu, Wu He, and Shancang Li. Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics*, 10(4):2233—-2243, Nov 2014.

[28] Laurence Yang, Beniamino Di Martino, and Qingchen Zhang. Internet of everything. *Mobile Information Systems*, 2017, Jul 2017.