IJCCN | INTERNATIONAL JOURNAL OF COMPUTING & COMMUNICATION NETWORKS

Vol. 2, Issue 1, February 2020

An overview of Internet of Things: Understanding the Issues and Challenges of a More Connected World

Abubakar Musa Ahmad[1], Ubaida Shehu Kalgo[1], Muhammad Saidu Aliero[2], Salisu Adamu Aliero[1]

[1]Kebbi State University of Science and Technology, Aliero, Nigeria

[2]School of IT Monash University Malaysia, Malaysia

* Corresponding Author: Muhammad Saidu Aliero, msaidua2000@gmail.com

Received; 25 September 2019, Revised; 25 October 2019, Accepted; 20 January 2020

Abstract: Internet of Things (IoT) is an emerging filed for technical, social, and economic significance. Consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and other everyday objects are being combined and connected with Internet and powerful data analytic capabilities that promise to transform the traditional services. Projection of IoT on the Internet and economy is impressive, with some anticipating as many as 100 billion connected IoT devices and a global economic impact of more than $11 trillion by 2025. At the same time, the IoT has been suffered from various challenges that need to be addressed with new standards, methods, and systems and provide more potential benefits. Attention-grabbing headlines about the hacking of Internet-connected devices, surveillance concerns, and privacy fears already have captured public attention. Technical challenges need new standards and policies, legal and development challenges need new methods and systems. This review paper presents a detail about current IoT challenges to help the new researchers in this area and filed to navigate the dialogue surrounding the IoT in the light of the competing predictions about its promises and perils.

Keywords: *IoT, Challenges, Security, Standards, Technical*

1. Introduction

Internet of Things (IoT) is an important area of research in toady's connected world. IoT networks and its applications have been gained popularity all over the world and one of the top areas of research [1-3]. This technology is based on a wide spectrum of wireless and wired enable products, systems, and sensors, which takes advantage of advanced computing capabilities, electronics miniaturization, and network interconnections to offer new

services. An abundance of conferences, reports, and news articles have discussed the prospects and impact of the "IoT revolution" for new market opportunities and business models with more security, privacy, and technical interoperability.

The large-scale implementation of IoT devices promises to transform many aspects of the way we live. For consumers, new IoT products like Internet-enabled appliances, home automation components, and energy management devices are moving us towards a vision of the "smart home'' and offering more security and energy efficiency capabilities [4]. Other personal IoT devices like wearable fitness and healthcare monitoring devices and network-enabled medical devices are transforming the way of traditional healthcare services [5, 6]. This technology has gained popularity and more beneficial for the elder and disabled people and improves their level of independence and quality of life at a reasonable cost. IoT systems like networked vehicles, intelligent traffic systems, and sensors embedded on roads and bridges move us closer to the idea of "smart cities'', which help to minimize the traffic congestion and energy consumption issues. IoT technology offers the possibility to transform the agriculture, industries, energy production, and distribution by increasing the availability of information. However, with various benefits, the IoT raises many issues and challenges that need to be considered and addressed for potential benefits.

Several companies and research organizations have offered a wide range of projections about the potential impact of IoT on the Internet and the economy during the next five to ten years. Cisco has launched more than 24 billion on Internet-connected objects by 2019; Morgan Stanley, however, projects 75 billion networked devices by 2020 [7]. Looking out further and raising the stakes higher, Huawei forecasts 100 billion IoT connections by 2025. McKinsey Global Institute suggests that the financial impact of IoT on the global economy may be as much as $3.9 to $11.1 trillion by 2025. While the variability in predictions makes any specific number questionable, collectively paint a picture of significant growth and influence.

Some observers see that the IoT as a revolutionary fully–interconnected "smart" world of progress, efficiency, and opportunity, with the potential for adding billions in value to industry and the global economy. Others warn that the IoT represents a darker world of surveillance, privacy and security violations, and consumer lock-in. Attention-grabbing headlines about the hacking of Internet-connected automobiles, surveillance concerns stemming from voice recognition features in "smart" TVs, and privacy fears stemming from the potential misuse of IoT data have captured public attention. This "promise vs. peril" debate along with an influx of information though popular media and marketing can make the IoT as one of a complex topic to understand.

Fundamentally, the Internet Society cares about the IoT as it represents a growing aspect of how people and institutions are likely to interact with the Internet in their personal, social, and economic lives. If even modest projections are correct, an explosion of IoT applications could present a fundamental shift in how users engage with and are impacted by the Internet, raising new issues and different dimensions of existing challenges across user/consumer concerns, technology, policy and law. IoT also has varying consequences in different economies and regions, bringing a diverse set of opportunities and challenges across the globe [8, 9].

This review paper helps the Internet society and community which navigates the dialogue surrounding the IoT in light of the competing predictions about its promises and perils. It provides a high-level overview of the basic IoT and some of the key issues and questions that this technology raises from the perspective of the Internet Society and the core values we promote. It also acknowledges some of the unique aspects of the IoT that make this a transformational technology for the Internet. As this is intended to be an overview document, we do not propose a specific course of action for ISOC on IoT at this time. Rather, we present an informational resource and starting point for discussion for the research community about IoT-related issues.

This paper is classified into three sections as follows:

- What is IoT? presents an overview of its origins, definitions, and technical connectivity models.
- What issues are raised by the IoT? And presents an introduction and discussion of concerns that have been raised.
- For further information, discusses the additional information and pointers to efforts around the world addressing IoT issues.

2. Internet of Things: Origins, Drivers, and Applications

The term "Internet of Things (IoT)" was first used in 1999 by British technology pioneer Kevin Ashton to described a system in which objects in the physical world could be connected to the Internet by sensors and actuators [10]. Ashton coined the term IoT to illustrates the power of connecting Radio-Frequency Identification (RFID) tags used in corporate supply chains to the Internet in order to count and track goods without the need for human intervention. Today, the IoT has become a popular term for describing scenarios in which Internet connectivity and computing capabilities extended to a variety of objects, devices, sensors, and everyday items.

While the term "IoT" is relatively new, where the concept of combining computers and networks are used to monitor and control the services. In the late 1970s, the traditional electric systems have used remotely for monitoring the meters via telephone lines. In the 1990s, advances in wireless technology allowed "machine–to–machine" (M2M) enterprise and industrial solutions for equipment monitoring and operation has become widespread. Many of these early M2M solutions are based on closed purpose-built networks and proprietary or industry-specific standards, rather than on Internet Protocol (IP) based networks and Internet standards.

Using IP to connect devices other than computers to the Internet is not a new idea. The first Internet "device" was an IP–enabled toaster that could be turned on and off over the Internet. It was featured at an Internet conference in 1990 [11]. Over the next several years, other "things" were IP–enabled, including a soda machine at Carnegie Mellon University in the US and a coffee pot in the Trojan Room at the University of Cambridge in the UK (which remained Internet connected until 2001) [12]. From these whimsical beginnings, a robust field of research and development into "smart object networking" create the foundation for today's IoT. If the idea of connecting objects to each other and to the Internet is not new, it is reasonable to ask, "Why is the IoT a newly popular topic today?".

From a broad perspective, the confluence of several technologies and market trends is making it possible to interconnect more and smaller devices. Some of the prominent features of IoT are as follows:

- **Ubiquitous Connectivity:** Low–cost, high–speed, pervasive network connectivity, especially through licensed and unlicensed wireless services and technologies, which makes it almost everything "connectable''.
- **Widespread Adoption of IP–based Networking:** IP has become the dominant global standard for networking, providing a well–defined and widely implemented platform of software and tools that can be incorporated into a broad range of devices easily and inexpensively.
- **Computing Economics:** Driven by industry investment in research, development, and manufacturing, Moore's law continues to deliver greater computing power at lower price points and lower power consumption.
- **Miniaturization:** Manufacturing advances allow cutting-edge computing and communications technology to be incorporated into very small objects. Coupled with greater computing economics, this has fueled the advancement of small and inexpensive sensor devices, which drive many IoT applications.
- **Advances in Data Analytics:** New algorithms and rapid increases in computing power, data storage, and cloud services enable the aggregation, correlation, and analysis of vast quantities of data; these large and dynamic datasets provide new opportunities for extracting information and knowledge.
- **Rise of Cloud Computing:** Cloud computing, which leverages remote, networked computing resources to process, manage, and store data, allows small and distributed devices to interact with powerful back-end analytic and control capabilities.

From this perspective, the IoT represents the convergence of a variety of computing and connectivity trends that have been evolving for many decades. At present, a wide range of industry sectors including automotive, healthcare, manufacturing, home and consumer electronics, and well beyond are considering the potential for incorporating IoT technology into their products, services, and operations [13]. Unlocking the potential of the IoT, the McKinsey Global Institute24 describes the broad range of potential applications in terms of "settings" where IoT is expected to create value for industries and users [14]. Table 1 shows the IoT applications and their area of usage.

Table 1: IoT Applications

S#	Area of Usage	Description	Examples
1	Human	Devices attached or inside the human body	Devices (wearables and ingestible) to monitor and maintain human health and wellness; disease management increased fitness and higher productivity.
2	Home	Buildings where people live	Home controllers and security systems
3	Retail Environments	Spaces where consumers engage in e-commerce	Stores, banks, restaurants, arenas anywhere consumers consider and buy; self-checkout, in-store, inventory optimization
4	Offices	Spaces where knowledge	Energy management and security in office buildings; improved productivity, including for mobile employees

		workers work	
5	Factories	Standardized production environments	Places with repetitive work routines, including hospitals and farms; operating efficiencies, optimizing equipment use and inventory
6	Worksites	Custom production environments	Mining, oil and gas, construction; operating efficiencies, predictive maintenance, health and safety
7	Vehicles	Systems inside moving vehicles	Vehicles including cars, trucks, ships, aircraft, and trains; condition-based maintenance, usage-based design, pre-sales analytics
8	Cities	Urban environment	Public spaces and infrastructure in urban settings; adaptive traffic control, smart meters, environmental monitoring, resource management
9	Outside	Between urban environments (and outside other settings)	Outside uses include railroad tracks, autonomous vehicles (outside urban locations), and flight navigation; real-time routing, connected navigation, shipment tracking

Many organizations have developed their taxonomies and categorizations of IoT applications and use cases. For example, “Industrial IoT’’ is a term widely used by companies and associations to describe IoT applications related to the production of goods and services, including manufacturing and utilities [15]. Others discuss IoT by device types, such as wearables and appliances. Still, others focus on IoT in the context of integrated location-based implementations such as “smart homes” or “smart cities’’. Whatever the application, it is clear that IoT use cases could extend to nearly every aspect of our lives [16].

As the number of Internet-connected devices grows, the amount of traffic they generate is expected to rise significantly. For example, Cisco estimates that Internet traffic generated by non-PC devices will rise from 40% in 2014 to just under 70% in 2019. Cisco also forecasts that the number of M2M connections (including in industrial, home, healthcare, automotive, and other IoT verticals) will rise from 24% of all connected devices in 2014 to 43% in 2019. One implication of these trends is that over the next ten years we could see a shift in the popular notion of what it means to be “on the Internet’’. The rapid growth of the worldwide web may have been just the trigger charge that is now setting off the real explosion, as things start to use the Internet [17, 18].

In the popular mindset, the world wide web has almost become synonymous with the Internet itself. Web technologies facilitate most interactions between people and content, making it a defining characteristic of the current Internet experience [19]. The web-based experience is largely characterized by the active engagement of users downloading and generating content through computers and smartphones. If the growth projections about IoT become reality, we may see a shift towards more passive Internet interaction by users with objects such as car components, home appliances, and self-monitoring devices; these devices send and receive data on the user’s behalf, with little human intervention or even awareness.

IoT may force a shift in thinking if the most common interaction with the Internet and the data derived and exchanged from that interaction comes from passive engagement with connected objects in the broader environment. The potential realization of this outcome a “hyper-connected world” is a testament to the general-purpose nature of the Internet architecture, which does not place inherent limitations on the applications or services that can make use of the technology.

2.1 Different Definitions and Similar Concepts

Despite the global buzz around the IoT, there is no single, universally accepted definition for the term IoT. Different definitions are used by various groups to describe or promote a particular view of what IoT means and its most important attributes. Some definitions specify the concept of the Internet or the IP, while others, perhaps surprisingly, do not. For example, consider the following definitions.

> “The Internet Architecture Board (IAB) begins RFC 7452, “Architectural Considerations in Smart Object Networking’’, with this description:

The term IoT denotes a trend where a large number of embedded devices employ communication services offered by Internet protocols. Many of these devices, often called "smart objects,’’ are not directly operated by humans, but exist as

components in buildings or vehicles, or are spread out in the environment. Within the Internet Engineering Task Force (IETF), the term "smart object networking" is commonly used in reference to the IoT. In this context, "smart objects" are devices that typically have significant constraints, such as limited power, memory, and processing resources, or bandwidth. Work in the IETF is organized around specific requirements to achieve network interoperability between several types of smart objects.

Published in 2012, the International Telecommunication Union (ITU) ITU–T Recommendation Y.2060, Overview of the IoT, discusses the concept of interconnectivity, but does not specifically tie the IoT to the Internet. A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

Note 1: Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

Note 2: From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3. Internet of Things Communications Models

From an operational perspective, it is useful to think about how IoT devices connect and communicate in terms of their technical communication models. In March 2015, the Internet Architecture Board (IAB) released a guiding architectural document for networking of smart objects (RFC 7452), which outlines a framework of four common communication models used by IoT devices. The discussion below presents this framework and explains key characteristics of each model.

3.1 Device-to-Device Communications

The device-to-device communication model represents two or more devices that directly connect and communicate between one another, rather than through an intermediary application server. These devices communicate over many types of networks, including IP networks or the Internet. Often, however these devices use protocols like Bluetooth, Wave, or ZigBee to establish direct device-to-device communications, as shown in Figure 1.

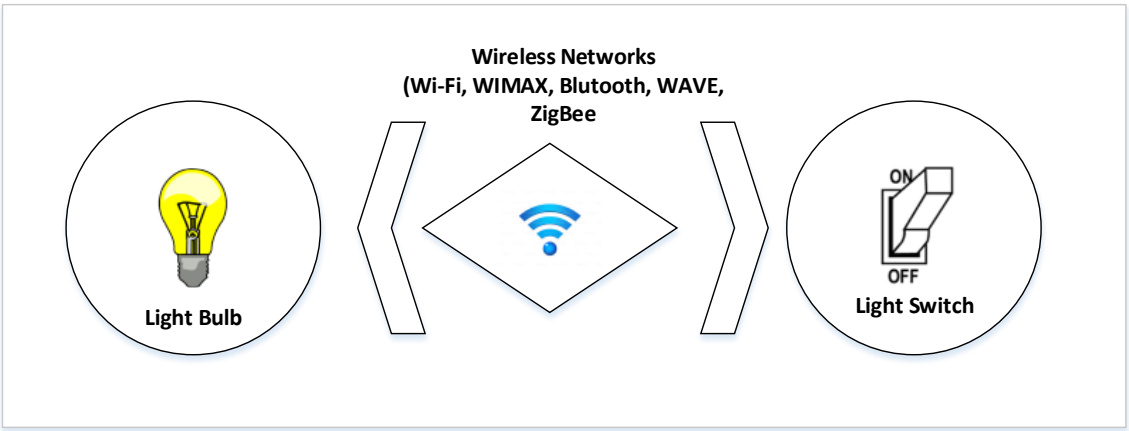

Figure 1. Example of device-to-device communication model

These device-to-device networks allow devices that adhere to a particular communication protocol to communicate and exchange messages to achieve their function. This communication model is commonly used in applications like home automation systems, which typically use small data packets of information to communicate between devices with relatively low data rate requirements. Residential IoT devices like light bulbs, light switches, thermostats, and door locks normally send small amounts of information to each other (e.g. a door lock status message or turn on light command) in a home automation scenario.

This device-to-device communication approach illustrates many of the interoperability challenges discussed later in this paper. As an IETF Journal article described, "these devices often have a direct relationship, they usually have built-in security and trust [mechanisms], but they also use device-specific data models that require redundant development efforts [by device manufacturers]" [20]. This means that device manufacturers need to invest in development efforts to implement device-specific data formats rather than open approaches that enable use of standard data formats.

From the user's point of view, this often means that underlying device-to-device communication protocols are not compatible, forcing the users to select a family of devices that employ a common protocol. For example, the family of devices using the wave protocol which is not natively compatible with the ZigBee family of devices. While these incompatibilities limit user choice to devices within a particular protocol family, the user benefits from knowing that products within a particular family tend to communicate well.

3.2 Device-to-Cloud Communications

In a device-to-cloud communication model, the IoT devices connect directly to an Internet cloud service like an application service provider to exchange data and control messages traffic. This approach frequently takes advantage of existing communications mechanisms like traditional wired Ethernet or Wi-Fi connections to establish a connection between the devices and the IP network, which ultimately connects to the cloud service. This communication model is employed by some popular consumer IoT devices like the Nest Labs. This is shown in Figure 2.

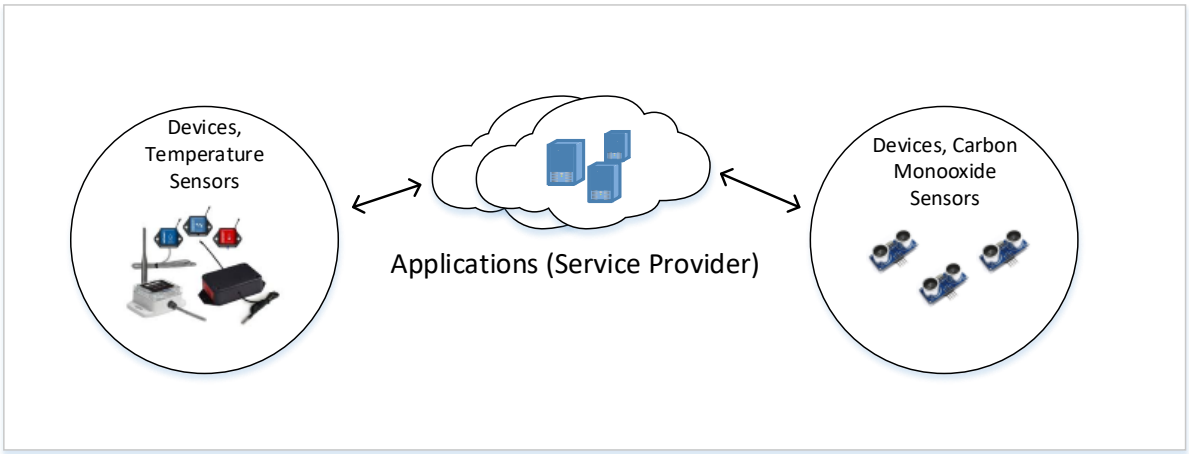

Figure 2. Device-to-cloud communication model diagram

In the case of Thermostat and the Samsung Smart TV, the devices transmit the data to a cloud database where the data can be used to analyze home energy consumption. Further, this cloud connection enables the user to obtains remote access to their thermostat via a smartphone or Web interface, and it also supports software updates to the thermostat. Similarly, with the Samsung Smart TV technology, the television uses an Internet connection to transmit user viewing information to Samsung for analysis and to enable the interactive voice recognition features of the TV. In these cases, the device-to-cloud model adds value to the end-user by extending the capabilities of the device beyond its native features [21]. However, interoperability challenges can arise when attempting to integrate devices made by different manufacturers. Frequently, the device and cloud service are from the same vendor. If proprietary data protocols are used between the device and the cloud service, the device owner or user may be tied to a specific cloud service, limiting or preventing the use of alternative service providers. This is commonly referred to as "vendor lock-in'', which is a term that encompasses other facets of the relationship with the provider such as ownership of and access to the data. At the same time, users can generally have confidence that devices designed for the specific platform can be integrated.

3.3 Device-to-Gateway Model

In the device-to-gateway model, or more typically, the device-to-application-layer gateway model, the IoT devices connect through service as a conduit to reach a cloud service. In simpler terms, this means that there is application software operating on a local gateway device, which acts as an intermediary between the device and the cloud service and provides security and other functionality such as data or protocol translation. The model is shown in Figure 3.

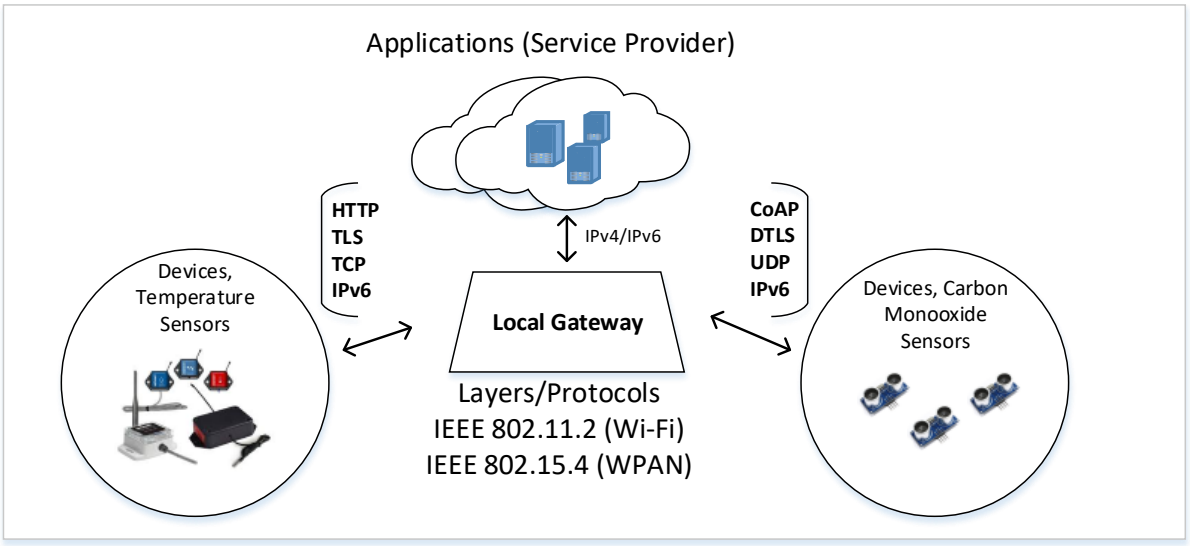

Figure 3. Device-to-gateway communication model diagram.

Several forms of this model are found in consumer devices. In many cases, the local gateway device is a smartphone running an app to communicate with a device and relay data to a cloud service. This is often the model employed with popular consumer items like personal fitness trackers. These devices do not have the native ability to connect directly to a cloud service, so they frequently rely on smartphone applications software to serve as an intermediary gateway to connect the fitness device to the cloud.

3.4 Back-End Data-Sharing Model

The back-end data-sharing model refers to a communication architecture that enables users to export and analyze smart object data from a cloud service in combination with data from other sources. This architecture supports "the users desire for granting access to the uploaded sensor data to third parties". This approach is an extension of the single device-to-cloud communication model, which can lead to data silos where "IoT devices upload data only to a single application service provider''. A back-end sharing architecture allows the data collected from single IoT device data streams to be aggregated and analyzed. For example, a corporate user in charge of an office complex would be interested in consolidating and analyzing the energy consumption and utility data produced by all the IoT sensors and Internet-enabled utility systems on the premises. Often in the single device-to-cloud model, the data of each IoT sensor or system produces sits in a stand-alone data. An effective back-end data sharing architecture would allow the company to easily access and analyze the data in the cloud produced by the whole spectrum of devices in the building [22]. Also, this kind of architecture facilitates data portability needs. Effective back-end data sharing architectures allow users to move their data when they switch between IoT services, breaking down traditional data silo barriers. The back-end data-sharing model suggests a federated cloud services approach or cloud Applications Programmer Interfaces (APIs) are needed to achieve interoperability of smart device data hosted in the cloud. A graphical representation of this design is shown in Figure 4.

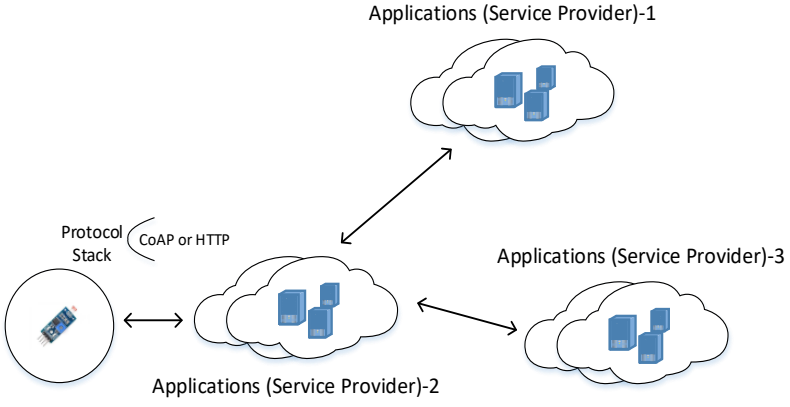

Figure 4. Back-end data sharing model diagram.

This architecture model is an approach to achieve interoperability among these back-end systems. As the IETF Journal suggests, "Standard protocols can help but are not sufficient to eliminate data silos because common information models are needed between the vendors." In other words, this communication model is only as effective as the underlying IoT system designs. Back-end data sharing architectures cannot fully overcome closed system designs.

3.5 Internet of Things Communications Models Summary

The four basic communication models demonstrated the underlying design strategies used to allow IoT devices to communicate. Aside from some technical considerations, the use of these models is largely influenced by the open versus proprietary nature of the IoT devices being networked. And in the case of the device-to-gateway model, its primary feature is its ability to overcome proprietary device restrictions in connecting IoT devices. This means that device interoperability and open standards are key considerations in the design and development of internetworked IoT systems. From a general user perspective, these communication models help to illustrates the ability of networked devices to add value to the end-user. By enabling the user to achieve better access to an IoT device and its data, the overall value of the device is amplified. For example, in three of the four communication models, the devices ultimately connect to data analytic services in a cloud computing setting. By creating data communication conduits to the cloud, users, and service providers can more readily employ data aggregation, big data analytics, data visualization, and predictive analytics technologies to get more value out of IoT data than can be achieved in traditional data-silo applications. In other words, effective communication architectures are an important driver of value to the end-user by opening possibilities of using the information in new ways. It should be noted, however, these networked benefits come with trade-offs. Careful consideration needs to be paid to the incurred cost burdens placed on users to connect to cloud resources when considering an architecture, especially in regions where user connectivity costs are high. While the end-user benefits from effective communication models, it should be mentioned that effective IoT communication models also enhance technological innovation and open opportunities for commercial growth. New products and services can be designed to take advantage of IoT data streams that didn't exist previously, acting as a catalyst for further innovation.

4. What issues are raised by the Internet of Things?

It would be impossible to cover the broad scope of issues surrounding the IoT in a single paper. We provide an overview of five topics frequently discussed in relation to IoT. These include security; privacy; interoperability and standards; legal, regulatory and rights; and emerging economies and development. We begin to examine these issues through the lens of "the Abilities", the statement of fundamental principles that guide ISOC's work in terms of the capabilities, we believe all Internet users should enjoy that must be protected. These include the ability to connect, speak, innovate, share, choose, and trust. With these principles as a guide, we present important aspects of each issue and propose several questions for discussion.

As we note, ensuring the security, reliability, resilience, and stability of Internet applications and services is critical to promoting trust and the use of the Internet. As users of the Internet, we need to have a high degree of trust that the Internet, its applications, and the devices linked to it are secure enough to do the kinds of activities we want to do online in relation to the risk tolerance associated with those activities. The IoT is different in this respect, and security in IoT is fundamentally linked to the ability of users to trust their environment. If people don't believe their connected devices and their information which are reasonably secure from misuse or harm, the resulting erosion of trust causes a reluctance to use the Internet. This has global consequences to electronic commerce, technical innovation, free speech, and practically every other aspect of online activities. Indeed, ensuring security in IoT products and services should be considered a top priority for this sector.

As we increasingly connect devices to the Internet, new opportunities to exploit potential security vulnerabilities grow. Poorly secured IoT devices could serve as entry points for cyberattacks by allowing malicious individuals to re-program a device or cause it to malfunction. Poorly designed devices can expose user data to theft by leaving data streams inadequately protected. Failing or malfunctioning devices also can create security vulnerabilities. These problems are just as large or larger for the small, cheap, and ubiquitous smart devices in the IoT as they are for the computers that have traditionally been the endpoints of Internet connectivity. Competitive cost and technical constraints on IoT devices challenge manufacturers to adequately design security features into these devices, potentially creating security and long-term maintainability vulnerabilities greater than their traditional computer counterparts. Along with potential security design deficiencies, the sheer increase in the number and nature of IoT devices could increase the opportunities for attack. When coupled with the highly interconnected nature of IoT devices, every poorly secured device that is connected online potentially affects the security and resilience of the Internet globally, not just locally. For example, an unprotected refrigerator or television in the US that is infected with malware might send thousands of harmful spam emails to recipients worldwide using the owner's home Wi-Fi Internet connection.

To complicate matters, our ability to function in our daily activities without using devices or systems that are Internet-enabled is likely to decrease in a hyperconnected world. In fact, it is increasingly difficult to purchase some devices that are not Internet-connected because certain vendors only make connected products. Day by day, we become more connected and dependent on IoT devices for essential services, and we need the devices to be secure, while recognizing that no device can be absolutely secure. This increasing level of dependence on IoT devices and the Internet services they interact with also increases the pathways for wrongdoers to gain access to devices. Perhaps we could unplug our Internet-connected TVs if they get compromised in a cyber-attack, but we can't so easily turn off a smart utility power meter or a traffic control system or a person's implanted pacemaker if they fall victim to malicious behavior. This is why security of IoT devices and services is a major discussion point and should be considered a critical issue. We increasingly depend on these devices for essential services, and their behavior may have global reach and impact.

4.1 A Spectrum of Security Considerations

When thinking about IoT devices, it is important to understand that the security of these devices is not absolute. IoT device security is not a binary proposition of secure or insecure. Instead, it is useful to conceptualize IoT security as a spectrum of device vulnerability. The spectrum ranges from totally unprotected devices with no security features to highly secure systems with multiple layers of security features. In an endless cat-and-mouse game, new security threats evolve, and device manufacturers and network operators continuously respond to address the new threats. The overall security and resilience of the IoT is a function of how security risks are assessed and managed [23]. Security of a device is a function of the risk that a device will be compromised, the damage such compromise will cause, and the time and resources required to achieve a certain level of protection. If a user cannot tolerate a high degree of a security risk as in the case of the operator of a traffic control system or person with an implanted, Internet-enabled medical device, then the user may feel justified in spending a considerable amount of resources to protect the system or device from attack. Likewise, if the user is not concerned that the refrigerator might be hacked and used to send spam messages, the user may not feel compelled to pay for a model that has a more sophisticated security design if it makes the device costly or complicated.

Several factors influence this risk assessment and mitigation calculation. Factors include having a clear understanding of the present security risks and the potential future risks; the estimated economic and other costs risks are realized, and the estimated cost to mitigate the risks. While these kinds of security trade-offs are often made from an individual user or organizational perspective, it is also important to consider the interrelatedness of IoT devices as part of a larger IoT ecosystem. The networked connectivity of IoT devices means that security decisions made locally about an IoT device can have global impacts on other devices. As a matter of principle, developers of smart objects for the IoT have an obligation in ensuring that those devices do not expose either their own users or others to potential harm [24]. As a matter of business and economics, vendors have an interest in reducing their cost, complexity, and time to market. For example, IoT devices that are high–volume, low–margin components that already represent a cost added to that of the product in which they are embedded are becoming quite common; adding more memory and a faster processor to implement security measures could easily make that product commercially uncompetitive.

In economic terms, lack of security for IoT devices results in a negative externality, where a cost is imposed by one party (or parties) on other parties. A classic example is the pollution of the environment, where the environmental damage and cleanup costs (negative externalities) of a polluter's actions are borne by other parties. The issue is that the cost of the externality imposed on others is not normally factored into the decision-making process, unless, as is the case with pollution, a tax is imposed on the polluter to convince him to lower the amount of pollution [25]. In the case of information security, an externality arises when the vendor creating the product does not bear the costs caused by any insecurity; in this case, liability law can influence vendors to account for the externality and develop more security products. These security considerations are not new in the context of information technology, but the scale of unique challenges that can arise in IoT implementations, as described below, make them significant.

4.2 Unique Security Challenges of IoT Devices

IoT devices tend to differ from traditional computers and computing devices in important ways that have been facing security challenges as follows:

- Many IoT devices, such as sensors and consumer items, are designed to be deployed at a massive scale that is orders of magnitude beyond that of traditional Internet-connected devices.

As a result, the potential quantity of interconnected links between these devices is unprecedented. Further, many of these devices will be able to establish links and communicate with other devices on their own in an unpredictable and dynamic fashion. Therefore, existing tools, methods, and strategies associated with IoT security may need new consideration.

- Many IoT deployments will consist of collections of identical or near-identical devices. This homogeneity magnifies the potential impact of any single security vulnerability by the sheer number of devices that all have the same characteristics. For example, a communication protocol vulnerability of one company's brand of Internet-enabled light bulbs might extend to every make and model of device that uses that same protocol or which shares key design or manufacturing characteristics.
- Many IoT devices will be deployed with an anticipated service life many years longer than is typically associated with high-tech equipment. Further, these devices might be deployed in circumstances that make it difficult or impossible to reconfigure or upgrade them; or these devices might outlive the company that created them, leaving orphaned devices with no means of long-term support. These scenarios illustrate that security mechanisms that are adequate where deployment might not be adequate for the full lifespan of the device as security threats evolve. As such, this may create vulnerabilities that could persist for a long time. This is in contrast to the paradigm of traditional computer systems that are normally upgraded with operating system software updates throughout the life of the computer to address security threats. The long-term support and management of IoT devices have a significant security challenge.
- Many IoT devices are intentionally designed without any ability to be upgraded, or the upgrade process is cumbersome or impractical. For example, consider the 2015 Fiat Chrysler recall of 1.4 million vehicles to fix a vulnerability that allowed an attacker to wirelessly hack into the vehicle. These cars must be taken to a Fiat Chrysler dealer for a manual upgrade, or the owner must perform the upgrade themselves with a USB key.

5. Conclusion

While the concept of combining computers, sensors, and networks to monitor and control devices has been around for decades, the recent confluence of key technologies and market trends is ushering in a new reality for the "Internet of Things''. IoT promises to usher in a revolutionary, fully interconnected "smart" world, with relationships between objects and their environment and objects and people becoming more tightly intertwined. The prospect of the IoT is a ubiquitous array of devices bound to the Internet which might fundamentally change how people think about what it means to be "online". While the potential ramifications are significant, a number of potential challenges may stand in the way of this vision, particularly in the areas of security; privacy; interoperability and standards; legal, regulatory, and rights issues; and the inclusion of emerging economies. The IoT involves a complex and evolving set of technological, social, and policy considerations across a diverse set of stakeholders. The IoT is happening now, and there is a need to address its challenges and maximize its benefits while reducing its risks. The Internet society cares about IoT because it represents a growing aspect of how people and institutions are likely to interact with and incorporate the Internet and network connectivity into their personal, social, and economic lives. Solutions to maximizing the benefits of IoT while minimizing the risks will not be found by engaging in a polarized debate that pits the promises of IoT against its possible perils. Rather, it will take informed engagement, dialogue, and collaboration across a range of stakeholders to plot the most effective ways forward. In the future, we will consider the other challenges and try to review in more depth.

References

[1] M. C. Domingo, "An overview of the Internet of Things for people with disabilities," *Journal of Network Computer Applications,* vol. 35, no. 2, pp. 584-596, 2012.

[2] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems,* vol. 82, pp. 395-411, 2018.

[3] K. N. Qureshi, A. H. Abdullah, F. Bashir, S. Iqbal, and K. M. Awan, "Cluster-based data dissemination, cluster head formation under sparse, and dense traffic conditions for vehicular ad hoc networks," *International Journal of Communication Systems,* vol. 31, no. 8, p. e3533, 2018.

[4] A.-R. Al-Ali, I. A. Zualkernan, M. Rashid, R. Gupta, and M. Alikarar, "A smart home energy management system using IoT and big data analytics approach," *IEEE Transactions on Consumer Electronics,* vol. 63, no. 4, pp. 426-434, 2017.

[5] Y. Zia, A. Farhad, F. Bashir, K. N. Qureshi, and G. Ahmed, "Content-based dynamic superframe adaptation for Internet of Medical Things," *International Journal of Distributed Sensor Networks,* vol. 16, no. 2, p. 1550147720907032, 2020.

[6] K. N. Qureshi, M. M. Idrees, J. Lloret, and I. Bosch, "Self-Assessment Based Clustering Data Dissemination for Sparse and Dense Traffic Conditions for Internet of Vehicles," *IEEE Access,* vol. 8, pp. 10363-10372, 2020.

[7] S. K. Lee, M. Bae, and H. Kim, "Future of IoT networks: A survey," *Applied Sciences*, vol. 7, no. 10, p. 1072, 2017.
[8] 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.
[9] S. Tang, D. R. Shelden, C. M. Eastman, P. Pishdad-Bozorgi, and X. Gao, "A review of building information modeling (BIM) and the internet of things (IoT) devices integration: Present status and future trends," *Automation in Construction*, vol. 101, pp. 127-139, 2019.
[10] T. Kramp, R. Van Kranenburg, and S. Lange, "Introduction to the Internet of Things," in *Enabling Things to Talk*: Springer, Berlin, Heidelberg, 2013, pp. 1-10.
[11] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. Aswathy, "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," in *2014 International conference on science engineering and management research (ICSEMR)*, 2014, pp. 1-8: IEEE.
[12] N. Sharma, M. Shamkuwar, and I. Singh, "The history, present and future with IoT," in *Internet of Things and Big Data Analytics for Smart Generation*: Springer, 2019, pp. 27-51.
[13] K. N. Qureshi, A. Ahmad, F. Piccialli, G. Casolla, and G. Jeon, "Nature-inspired algorithm-based secure data dissemination framework for smart city networks," *Neural Computing and Applications*, 2020/04/10 2020.
[14] K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview," *The Internet Society (ISOC)*, vol. 80, pp. 1-50, 2015.
[15] K. N. Qureshi, S. S. Rana, A. Ahmed, and G. Jeon, "A Novel and Secure Attacks Detection Framework for Smart Cities Industrial Internet of Things," *Sustainable Cities and Society*, p. 102343, 2020.
[16] C. X. Mavromoustakis, G. Mastorakis, and J. M. Batalla, *Internet of Things (IoT) in 5G mobile technologies*. Springer, 2016.
[17] F. Al-Turjman, "5G-enabled devices and smart-spaces in social-IoT: an overview," *Future Generation Computer Systems*, vol. 92, pp. 732-744, 2019.
[18] K. N. Qureshi and A. H. Abdullah, "Industrial Wireless Sensor Network Architecture Standards, Applications," in *AsiaSense, the sixth international conference 2013, Melaka, Malaysia*, 2013: AaiaSense.
[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] R.-W. Bello, "Societal Adoption problems of Internet of Things (IOT)-A Study," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 8, no. 9, pp. 5-11, 2018.
[21] J. Byun, S. Kim, J. Sa, S. Kim, Y.-T. Shin, and J.-B. Kim, "Smart city implementation models based on IoT technology," *Advanced Science and Technology Letters*, vol. 129, no. 41, pp. 209-212, 2016.
[22] J. Ju, M.-S. Kim, and J.-H. Ahn, "Prototyping business models for IoT service," *Procedia Computer Science*, vol. 91, pp. 882-890, 2016.
[23] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," ed: Elsevier, 2018.
[24] C. Patel and N. Doshi, "Security challenges in IoT cyber world," in *Security in Smart Cities: Models, Applications, and Challenges*: Springer, 2019, pp. 171-191.
[25] H. R. Ghorbani and M. H. Ahmadzadegan, "Security challenges in internet of things: survey," in *2017 IEEE Conference on Wireless Sensors (ICWiSe)*, 2017, pp. 1-6: IEEE.