International Journal of Hyperconnectivity and the Internet of Things
Volume 2 • Issue 1 • January-June 2018

The Internet of Things:
Enabling Artificial Intelligence

Mohamed A Eltayeb, Bellevue University, Bellevue, USA

ABSTRACT

In recent years, the Internet of Things (IoT) has become an increasingly prominent concept, and the benefits associated with this technology are seemingly limitless. The interest in the IoT stems from its elasticity and scalability and scholars, researchers, and investors alike are increasingly turning their attention to how best to harness this powerful concept. One area that has become of specific interest relates to the vast amount of data that is generated by the sensors that form the diverse networks that sit at the core of the IoT. More and more opportunities to collate and harness this data are emerging, and the collection of intelligence can be of significant value politically, economically, and socially. This article hence examines some of the ways in which the IoT can be employed to advance the artificial intelligence (AI). Furthermore, this article presents and discusses the limitations of the current systems and propose recommendations for the future direction.

KEYWORDS

Artificial Intelligence, Enabling Intelligence, Internet of Things, RFID Technology

DOI: 10.4018/IJHIoT.2018010101

INTRODUCTION

Modern-day society is replete with technologies and communication systems, and we are surrounded by a complex web of devices, sensors, and other physical components that are utilized to compile and exchange information. In fact, according to Eltayeb (2016), the majority of objects that we use on a daily basis will be connected to the IoT network in some shape or form in the near future. The IoT is a very promising concept that has attracted significant attention from contemporary scholars due to its highly scalable and agile nature. This concept has undergone rapid transformations since it was initially introduced, and it now has a fundamental influence on business, industry, and society.

The 2017 Hype Cycle, presented three distinct technology trends: Artificial Intelligence (AI) everywhere, transparently immersive experiences and digital platforms. These three technology trends create new experiences with the unrivaled intelligence (Panetta, 2017). Analysts predict that around 50 billion new objects will be introduced to the IoT network by the year 2020 (Nguyen & Simkin, 2017). As more sensors, components, and devices are added to the network, data collection will grow exponentially, and this data will result in the generation of intelligence that has significant political, economic, industrial, and social value.

While the IoT is a complex technology, its fundamental function is allowing us to track, collate, transmit, and share large amounts of data and information. The intelligence gathered by these systems holds significant potential, and it is widely acknowledged that the ongoing proliferation of IoT will result in the automation of many everyday tasks. This article hence presents a detailed overview of the ways in which the IoT operates and how it contributes to the development of Artificial Intelligence (AI).

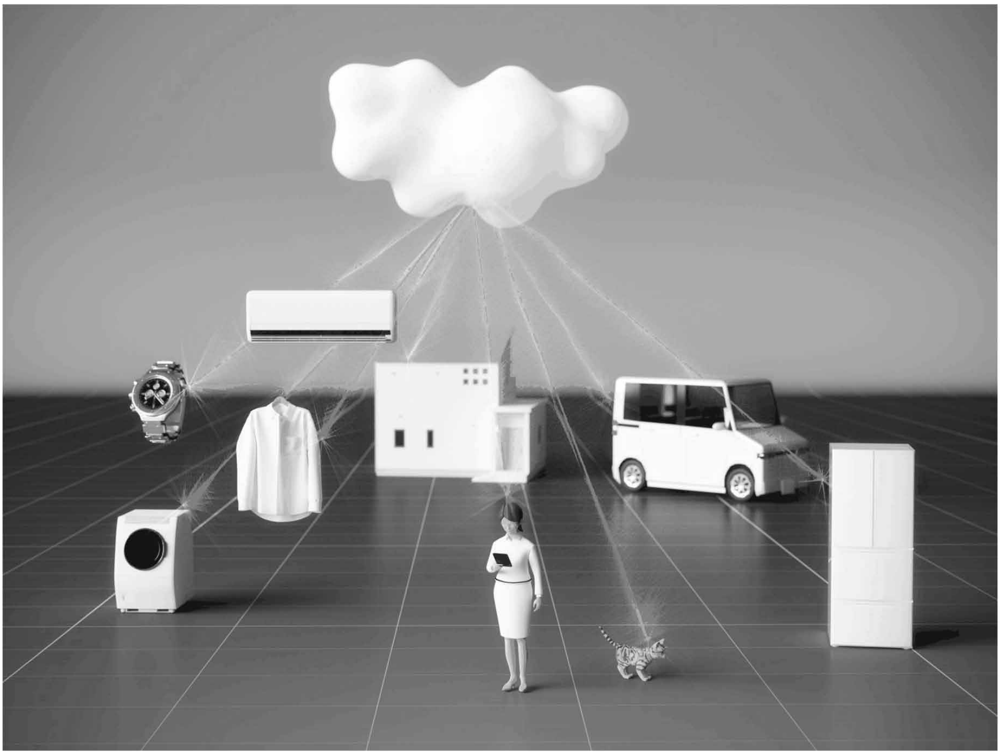
THE INTERNET OF EVERYTHING

The IoT has boundless potential. In its current form, the IoT consists of vast numbers of interconnected sensors that are embedded into everyday objects and systems that are subsequently distributed across a wide geographical and virtual web (Xia et al., 2012). These sensors are connected to one another via a virtual network that facilitates the collation and transmission of data (Eltayeb, 2017). The sheer reach and potential of the IoT and cloud computing in terms of its ability to facilitate communication and increase interaction entails that it holds significant potential for humanity on a social and industrial level. Figure 1 provides an overview of Internet of Things abstract concept.

WHAT IS THE IOT?

The IoT is a complex network of embedded sensors and other physical components that exchange data. It was initially conceived as a means of establishing a link between the virtual world and physical objects; however, since its introduction in 1999, its usage

Figure 1. IoT - abstract concept illustration



has become so wide and diverse that it is now an integral element of contemporary life. To understand the IoT better, it can be useful to think of it as a smart city. The city spans the world, and every basic component within it is connected to each other and is aware of what one another is doing and how it is functioning.

The IoT is in a continual state of evolution and has practical applications in a vast array of technologies, functions, and industries. In fact, its applications are becoming so widely spread that scholars predict sensors will be embedded in almost all everyday objects in the future. According to Maier (2016), the IoT market is extremely promising and will reach a value of up to $11.1 Trillion by 2025. The following subsections will examine the key concepts that underpin IoT technologies and assess the ways in which they facilitate the acquisition of intelligence.

Intelligent Sensors

Radio frequency identification (RFID) is at the heart of the IoT. RFID was initially introduced during the 1940s to facilitate military operations; as such, it is far from a novel technology. However, its ability to tag objects, track their behavior, and differentiate them from other objects holds enormous potential, and it has been used to great effect within many contemporary systems and environments. Examples of applications in which RFID has found use include security systems, supply chain and inventory management, parking tolls, and packaging. It has even been used to save lives. As RFID technologies continue to grow and develop, the use of RFID is only set to grow and, according to Mitrokotsa et al. (2010), it will permeate every aspect of human life as we know it in the future.

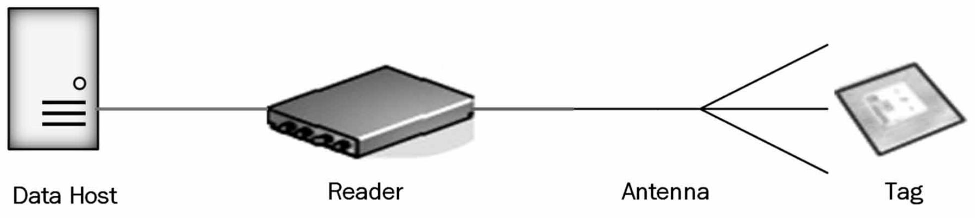
An RFID system consists of three fundamental parts: The tag (transponder), the reader (antenna), and the host computer (database/data processor). Each tag contains a very small microchip and a transmitter. The embedded transmitter sends an RFID signal, which is typically protected by network protocols, to the reader. The various components that can be found in a typical RFID system are shown in Figure 2.

The tag essentially acts as a unique identifier for the object to which it is linked. The reader accesses the information that is stored on the tag and subsequently transmits it to the host database. The host computer processes the information it receives from the reader by correlating the tag with its arbitrary records. RFIDs are currently employed in a wide variety of different applications; however, they can typically be classified into one of two types: active RFIDs and passive RFIDs. Active RFIDs contain a power source and their own transmitter, while passive RFIDs are activated remotely via a radio signal that is sent from the reader's antenna.

Intelligent Network (Wireless Sensor Networks)

Wireless sensor networks (WSN) are interconnected sensors that are scattered throughout different locations. Alcaraz et al. (2010) likened them to a "digital skin,"

Figure 2. RFID components



which forms a virtual layer through which computer systems access data from the physical world (p. 1). WSN are at the core of the operation of the IoT, and they work in collaboration with the sensor and RFID technologies to facilitate communication and connection between different objects: "The benefits of connecting both WSN and other IoT elements go beyond remote access, as heterogeneous information systems can be able to collaborate and provide common services" (Alcaraz et al., 2010, p. 1).

WSNs typically consist of a sensor, converter, communication unit, and a processor. The sensor nodes that form the WSN are interconnected with one or more host computers, and they collate and transmit information about the object's behavior, movements, and surroundings. All the data that the sensor nodes collect is transmitted to the sink node. A WSN makes it possible to collect and collate data from each respective node to perform detailed data collation and analysis at the sink level.

Smart Objects

The digital world is here now and, as such, the IoT is growing increasingly important for contemporary businesses. As a result of the development of the IoT systems and functionality, it is possible to attach practically any physical object to some form of sensor; for example, packages, pharmaceuticals, furniture, clothing, and animals. The more objects that are connected to the IoT, the more data that is acquired and, as such, the information that is available is growing at an exponential rate. Furthermore, the number of entry points to WSN are also increasing at a rapid rate (Perera et al., 2014).

The IoT connects everyday objects that incorporate sensors and collates and exchanges data between them. The interconnection of these objects allows them to be remotely controlled and managed. As such, it is largely anticipated that the sheer intelligence of the IoT will result in the efficient and accurate automation of many everyday tasks and fundamental changes in many industries and societies. To understand the basic concepts in more detail, it is worth assessing the way in which the IoT has facilitated information collection in contemporary society:

1. **Smart Home**

The IoT has simplified many of the tasks of everyday living and significantly reduced the effort it takes to manage the home. Feng (2017), described the IoT as "people-centric" and emphasized how it can deliver a smart home that is able to "enhance the intelligence level of the living environment and improve the quality of human life" (p.1). Via mobile phones, we can now control many different everyday items in the home, from the doors and windows to the heating and lighting systems. Some examples of home devices that commonly use the IoT are provided below:

- Ceiling fans: Ceiling fans are equipped with sensors that can monitor the temperature and humidity of a room and regulate the speed of the fan according to the required ambiance.

- Coffee maker: Smart coffee machines are connected to the Wi-Fi system, thereby allowing the user to control it from any location. It may send you a signal to let you know the water is running low or you can activate the machine from your bed first thing in the morning and have a steaming hot cup of coffee waiting for you by the time you reach the kitchen.
- Light bulbs: Smart lighting systems can sense when you enter the house and activate the bulbs accordingly. Some systems even claim to sense your mood and make appropriate lighting adjustments.

2. **Smart Government**

Within the government, the IoT can serve a variety of purposes. While it can be used to benefit citizens, if it is not managed properly, it may also be misused and has the potential to undermine liberties and peace. Some examples of potential applications of the IoT in government settings are outlined below:

- Collect and monitor classified information
- Track suspected terrorists' movements
- Improve military capabilities
- Enhance security levels
- Facilitate communication with the head of states of other countries

3. **Smart Enterprise**

The IoT has been used to great effect within many industrial contexts. One early use of RFID tags was in the retail industry, in which anti-theft devices were attached to stock to detect attempted theft. In mining companies, the IoT has been used to operate driverless vehicles that can work continuously without significant cost and reduce the risks workers are exposed to in the process of excavating a mine. Some examples of the functions that have benefitted from IoT-enabling intelligence in the enterprise setting are outlined below:

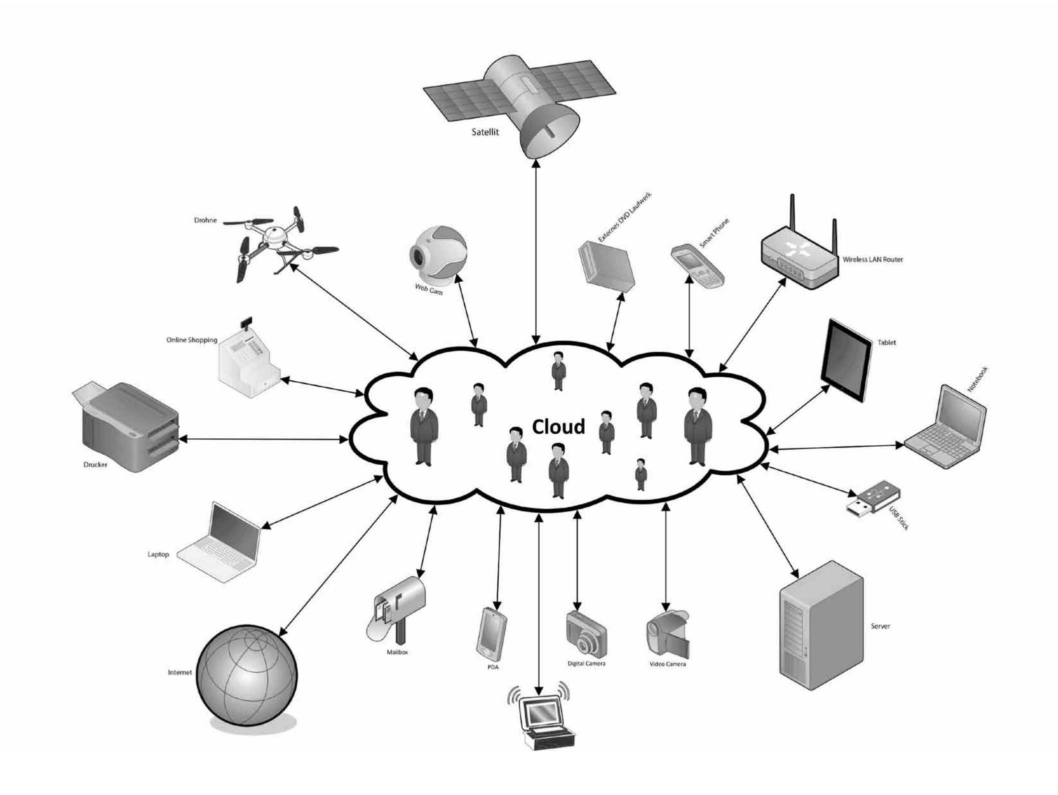
- To develop solutions to operational and internal challenges
- To develop unique business models
- To improve the growth of the entire enterprise by enhancing efficiency and reducing the cost of production
- To connect different organizations in such a way that they can share data and learn from one another.

Smart Cloud Computing

The combination of the IoT and cloud computing has led to really exciting changes in the last few years, and cloud computing is becoming increasingly important as a means of supporting the IoT. According to Saha et al. (2017), in combination, cloud computing and the IoT will shape the future of computing: "A strong framework of cloud computing, backed up by a seamless blending of sensors and actuators with the environment around us, is making this "network of networks of autonomous objects" a reality." (p.1). The relationship between the two technologies is relatively simple: The IoT captures the intelligence, while the cloud makes it possible to store, process, and analyze it.

We now find ourselves living in the midst of the information age, and this is fundamentally transforming everyday life as we know it. The IoT and cloud computing have found extensive application in both businesses and personal contexts and is helping people to experience agiler, mobile lives. People now live their lives online and demand access to data, emails, music, videos, games, and other applications when and where they need it (see figure 3). The need for instantly accessible media has led to the emergence of cloud clients and hosts, which include the likes of Dropbox, Google Music Service, iCloud, and SkyDrive (Eltayeb, 2014). However, demands are evolving, and people are now seeking approaches by which they can use mobile technology to achieve even more feats: "Mobile apps can integrate sensors and actuators in Internet-of-Things systems to achieve novel and diverse functionalities" (p. 1). To better understand the relationship between cloud computing and the IoT, it is worth briefly examining the development of Cloud Computing.

Figure 3. Smart Cloud Computing – Information-Centric



RECOMMENDATIONS AND FUTURE DIRECTIONS

Although the IoT has immense potential for the future, it is not without its drawbacks. As much as IoT can be beneficial, it is also a source of much harm. One of the biggest issues that is currently associated with the IoT is security. Hackers have a significant interest in the vast volumes of information that is collected in stored in the cloud and hardly a day goes by without reports of theft, misuse, or ethical issues associated with cloud resources.

A number of studies have highlighted the important role that user trust plays in the adoption of technologies (Sicari et al., 2015; Yan et al., 2014; Habib et al., 2014; Rivard, & Lapointe, 2012). Hence, for the IoT to achieve its full potential, it is imperative that providers establish methods of ensuring the data that is collected for IA is safe and that users' privacy is fully protected at all times. Providers have to take full accountability for protecting users' rights, acting responsibly, and ensuring their information is never leaked.

To effectively deploy the IoT, it is essential that the demands of the consumers of collected data and intelligence are balanced with the rights of those whose personal data is being acquired to contribute to the global intelligence. To achieve this balance, standardized processes and methods need to be developed by which the data that is used is carefully monitored and protected.

The provision of an IoT that consumers trust depends on a provider's ability to create private and secure systems that utilize best practices. A global set of rules and expectations need to be established that govern the provision of these services. At present, legislation in this area is lacking, and many countries have no solid regulations in place regarding the use and provision of the IoT.

The manufacturers of the hardware and software components that are required for the IoT need to take accountability for addressing privacy and safety exposures and to better understand the impact that their decisions have on consumer satisfaction. According to Weber (2010), the main privacy and security issues that need to be considered when providing the IoT systems are as follows:

- The need for an intelligent system that can respond to attack and adjust itself to node failures.
- **Robust Data Authentication:** There is a basic need to authenticate access to object information.
- **Access Control:** Stringent access control procedures need to be in place to ensure the data is only accessed by those with authority to do so.
- **Client Privacy:** The ability to link customers with data should be eradicated.

CONCLUSION

This article presented a detailed overview of the technological developments that have facilitated the evolution of intelligence technologies. The underlying concepts of the IoT was explored and its contemporary applications were examined. The limitations of the current systems were highlighted and recommendations for the future direction of these technologies were proposed.

REFERENCES

Alcaraz, C., Najera, P., Lopez, J., & Roman, R. (2010, November). Wireless sensor networks and the internet of things: Do we need a complete integration? In *1st International Workshop on the Security of the Internet of Things (SecIoT'10).*

Eltayeb, M. (2016). Privacy and Security. *Security Solutions for Hyperconnectivity and the Internet of Things*, *89*.

Eltayeb, M. A. (2017). Internet of Things: Privacy and Security Implications. *International Journal of Hyperconnectivity and the Internet of Things*, *1*(1), 1–18. doi:10.4018/IJHIoT.2017010101

Feng, S., Setoodeh, P., & Haykin, S. (2017). Smart Home: Cognitive Interactive People-Centric Internet of Things. *IEEE Communications Magazine*, *55*(2), 34–39. doi:10.1109/MCOM.2017.1600682CM

Habib, S. M., Ries, S., Mühlhäuser, M., & Varikkattu, P. (2014). Towards a trust management system for Cloud Computing marketplaces: Using caiq as a trust information source. *Security and Communication Networks*, *7*(11), 2185–2200. doi:10.1002/sec.748

Han, Y., Sun, J., Wang, G., & Li, H. (2010). A Cloud-based BPM architecture with user-end distribution of non-compute-intensive activities and sensitive data. *Journal of Computer Science and Technology*, *25*(6), 1157–1167. doi:10.1007/s11390-010-9396-z

Maier, M. V. (2016). The Internet of Things (IoT): what is the potential of Internet of Things applications for consumer marketing? [Bachelor's thesis]. University of Twente.

Mitrokotsa, A., Rieback, M. R., & Tanenbaum, A. S. (2010). Classifying RFID attacks and defenses. *Information Systems Frontiers*, *12*(5), 491–505. doi:10.1007/s10796-009-9210-z

Nguyen, B., & Simkin, L. (2017). The Internet of Things (IoT) and marketing: the state of play, future trends and the implications for marketing.

Okezie, C. C., Chidiebele, U. C., & Kennedy, O. C. (2012). Cloud Computing: A cost effective approach to enterprise web application implementation (A case for Cloud ERP web model). *Academic Research International*, *3*(1), 432–443.

Panetta, C. K. (2017, August 15). Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017. Retrieved March 12, 2018, from https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context aware Computing for the internet of things: A survey. *IEEE Communications Surveys and Tutorials*, *16*(1), 414–456. doi:10.1109/SURV.2013.042313.00197

Rivard, S., & Lapointe, L. (2012). Information technology implementers' responses to user resistance: Nature and effects. *Management Information Systems Quarterly*, *36*(3), 897–920.

Saha, H. N., Mandal, A., & Sinha, A. (2017, January). Recent trends in the Internet of Things. In *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 1-4). IEEE. doi:10.1109/CCWC.2017.7868439

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–166. doi:10.1016/j.comnet.2014.11.008

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23–30. doi:10.1016/j.clsr.2009.11.008

Xia, F., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of things. *International Journal of Communication Systems*, *25*(9), 1101–1102. doi:10.1002/dac.2417

Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications*, *42*, 120–136. doi:10.1016/j.jnca.2014.01.014

Mohamed Eltayeb is a dependable, conscientious, and enthusiastic engineer who possesses a wealth of comprehensive experience working with complex technologies from the early stages of design through to post-implementation adaptation. His research specializes in the areas of cloud computing, The Internet of Things, cyber security, artificial intelligence, information assurance, and mobile computing. His research efforts to date have specifically focused on examining the user acceptance of new technologies, and he has conducted detailed and comprehensive analysis of user acceptance in the domain of cloud computing