The Internet of Everything: Weighing Better Insights Against Information Security

Justin Wasser

University of Maryland Global Campus

ITEC 626: Information Systems Infrastructure

Professor Henson

10/11/2022

Abstract

The purpose of the following research paper is to examine The Internet of Everything (IoE), including its four main components, the synergetic effect created by connecting these components, as well as the benefits and concerns the IoE presents. Furthermore, conclusions drawn about where the IoE is likely headed in the near future will drive the purchase recommendations I would make for a client.

Introduction

As an expert trusted with the task of advising a client on technology-related purchases, it was necessary to examine state-of-the-art Internet of Everything technology/capabilities as well as examine the relationship between its underlying components to make accurate predictions regarding how the IoE will evolve in the near future. For those reasons, it is necessary to analyze the four main components that constitute The Internet of Everything, IoE's benefits, and the risks IoE introduces to information systems with respect to leveraging the IoE. Lastly, conclusions reached from the ensuing analysis will inform the technology purchase recommendations prepared for a client.

The Internet of Everything (IoE)

The Internet of Everything will continue to evolve and gain access to more data covering an ever-increasing range of processes, which in turn will enable better insights into all aspects of human activities (Gacovski, 2019; Liu et al., 2020). These insights generated by the IoE will lead to the creation of intelligence that will far surpass those that humans or machines have been capable of producing to this point in society's history (Liu et al., 2020). However, the increased connectivity created by the IoE will introduce new avenues for gaining unauthorized access to enterprise information systems (Karie et al., 2021). Therefore, businesses that can balance the utilization of the intelligence created by the IoE with appropriate information security control procedures are the ones that will thrive in the near future. Therefore, I recommend that my client purchase a "3 year standard reserved Instance" (Amazon Web Services, n.d.) to perform a dedicated, IoE-enabled, analysis of the company's business processes and operations. Furthermore, I would recommend my client purchase and provide employees with company-issued devices and require that only those devices be used when accessing enterprise information systems.

Several topics must be considered to illustrate why the IoE will lead to new and difficult information security challenges for enterprise information systems. Those topics include IoE's "four pillars" (Liu et al., 2020 pg. 67), a sampling of present-day and near-future IoE-enabled applications, and the challenge that securing information transmitted by IoT devices presents. The Internet of Everything can be defined as a technological concept consisting of four separate components that become The Internet of Everything when those aforementioned components begin to interface with one another (Liu et al., 2020). To that point, the "four pillars" (Liu et al., 2020) of the IoE that need to coalesce with one another in order to form The Internet of Everything include "people, data, process, and things" (Liu et al., 2020, pg. 67). These components define what constitutes The Internet of Everything, and therefore it is necessary to examine them further. Furthermore, an examination of The Internet of Things (IoT) is a logical starting point as it acts as the main infrastructure upon which the IoE is built (Liu et al., 2020).

IoE's Four Components

The Internet of Things (IoT) can be defined as a wide range of devices that are connected to the internet and through that connection to the internet become 'smart' (Liu et al., 2020). Just a few examples of common smart devices or applications contained within the IoT umbrella include smartphones, smart watches, self-driving cars, smart thermostats, and smart sensors (Gacovski, 2019). Furthermore, The Internet of Things (IoT) consisting of the aforementioned smart devices has evolved to essentially become the nodes within the larger framework that is The Internet of Everything (Jagatheesaperumal et al., 2022). For that reason, it makes perfect sense why The Internet of Everything is termed as it is, as any device that can send and receive data via a connection to the internet has the potential to be part of the IoE (Gacovski, 2019). Additionally, it is crucial to note that how the data generated from IoT devices is used determines whether the

device is part of the IoE. When data collected from IoT devices is transmitted with the ultimate goal of improving human-related processes it can be considered part of the IoE (Liu et al., 2020).

As mentioned in the preceding paragraph, The Internet of Everything relies on IoT devices as nodes to gather and transmit data (Liu et al., 2020). Furthermore, the scope and scale of data being gathered by IoT devices are expected to continue to grow at a rapid pace in the near future due to the ever-increasing number of IoT devices, combined with the rising connectivity between those devices (Gacovski, 2019). It is likely impossible to accurately predict just how large an increase in data traffic there may be in the near future (5-10 years), but looking at recent trends is one method often used to get a sense of potential coming growth. To that point, "this trend looks set to continue with data traffic from IoT devices rising from 2% share of the total in 2013 to 17% in 2020" (Gacovski, 2019, pg. 66). Moreover, this represents a 750% increase in IoT data traffic over an eight-year period, which averages out to approximately a 94% growth rate per year (Gacovski, 2019). Therefore, it can be safely assumed that IoT data traffic will continue to grow exponentially in the near future, now the question becomes how the IoE leverages this vast ocean of data.

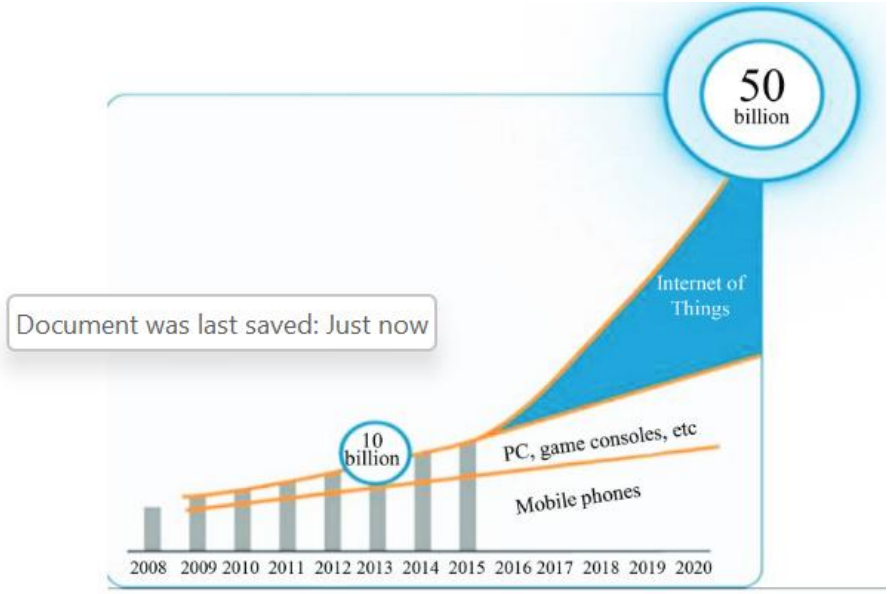

Figure 1: Device distribution in IoT [2] .

(Gacovski, 2019, pg. 66)

The answer to the question posed above is that the IoE will use the enormous amount of data gathered to synthesize better processes for everything it is attached to (Liu et al., 2020). The way the IoE will accomplish that is through a variety of artificial intelligence (AI) algorithms that have been developed to draw insights from big data (Liu et al., 2020). Some of the AI algorithms used for IoE data analysis include "machine learning (ML) deep learning (DL), reinforcement learning (RL), computer vision (CV), recommendation system (RS), knowledge graph (KG), and collective intelligence (CL, similar to swarm intelligence)" (Liu et al., 2020, pg. 69). At this point a brief remark should be made on the relationship between smart devices and intelligence as they are applied in the context of smart devices (IoT) and the IoE. The term smart device can be slightly misleading as it can facilitate the discovery of insights (intelligence) based on the data it gathers, but those insights are significantly limited by siloed nature of a smart device and its limited computational power. However, the IoE frees IoT devices from their limitations by creating a

collective entity consisting of the data gathered from all IoT devices, and all of the computing resources connected to the internet (Liu et al., 2020). Furthermore, the IoE leverages those two resources to produce insights that lead to the creation of more intelligent processes (Liu et al., 2020). Finally, the creation of more intelligent processes illuminates the last component of The Internet of Everything, people, as improving the lives of people is the IoE's ultimate goal (Dey et al., 2019).

Improving the quality of people's lives, and the advancement of humanity are the reasons for the birth of the IoE, so it is only logical that The Internet of Everything begins and ends with people (Liu et al., 2020). People are the ones who use smartphones, wear smartwatches, drive (or use) smart cars, and buy commercial products (assisted by the Industrial Internet of Things (IIoT)) (Hu et al., 2022). Furthermore, people are the group that ultimately benefits from being a part of the IoE system (Liu et al., 2020). Therefore, an examination of how exactly this benefit to humanity is achieved by The Internet of Everything is required.

The Evolution of the IoT Into the IoE

It can be helpful to conceptualize The Internet of Everything as growing from The Internet of Things, which acted as a petri dish of sorts for the IoE's evolution (Liu et al., 2020). Furthermore, this characterization also holds when examining IoT's and IoE's respective goals, as the goal of IoT is to "connect everything to everything to collect data and obtain analytical results from that data to make an intelligent system" (Dey et al., 2019, pg. 52). The IoE's goal simply expands the scope of data collection and analysis to include benefits to individual people, as well as society as a whole (Liu et al., 2020).

The way that the IoE accomplishes its goal is by gathering data on human issues and analyzing it in the same way IoT would for an issue between machines (Liu et al., 2020). The Internet of Everything seeks to leverage IoT-generated data to produce the highest quality of intelligence regarding human activities such as transportation, food production, healthcare, etc. to improve their related processes (Marjani et al., 2017). Additional benefits resulting from the growth of the IoE are increased connectivity between humans and technology, as well as increased connectivity between people (TEDx Talks, 2021). Moreover, this increased level of connectivity enables new data points to be mapped, which in turn enables new intelligence to be gained (TEDx Talks, 2021). Furthermore, as the previous point exemplified, the potential of The Internet of Everything is exponential in nature as everything connected to it can tap into the entire IoE repository of knowledge, while the IoE's intelligence is furthered with each new data point (person or IoT) it is connected to (Evans, 2012). Finally, humanity is already beginning to see the benefits of the IoE in the form of current and near-future applications.

Current & Near-Future IoE Applications

An example of a state-of-the-art use of the IoE is a healthcare application referred to as an "ambient intelligence (AmI) system" (Dey et al., 2019, pg. 137). This system combines the knowledge produced by multiple IoT devices including "biometric sensors, a wearable sensor, motion detection sensor and implantable sensors" (Dey et al., 2019, pg. 137) to produce a greater understanding of patients' health than isolated IoT sensors/devices could on their own (Dey et al., 2019). Furthermore, the connected framework exemplified by the ambient intelligence system is being used for a great many near-future IoE-enabled applications.

For instance, research is being conducted on how the Internet of Everything framework can be leveraged to create an "Urban Flooding Surveillance System" (Dhaya et al., 2022, pg. 1).

Furthermore, the system will make use of many technologies including IoT sensors, simulation models, cloud computing, and data transfer protocols, all of which are connected and through that connection are made exponentially more impactful (Dhaya et al., 2022). Additionally, the proposed flooding surveillance system will lead to better intelligence regarding flood patterns, which will directly lead to earlier warnings for people in the areas that will be affected (Dhaya et al., 2022). Finally, the implementation of the proposed "Cloud-Based IoE Enabled…Urban Flooding Surveillance System" (Dhaya et al., 2022, pg. 1), is an example of how the IoE can be leveraged to improve a process, which results in improving the quality of life of people affected by that process. However, for The Internet of Everything to reach its potential, it needs to be able to account for one of the greatest weaknesses inherent in its architecture, humans.

As currently constructed, humans present a significant challenge to "human-in-the-loop" (Maghsudi & Davy, 2020, pg. 1) IoE-enabled systems, because human decision-making is fallible in its nature (Maghsudi & Davy, 2020). In particular, human beings' decision-making can be impacted by several different factors, including "inaccurate beliefs and imprecise predictions; (ii) Humans often act irrationally and based on heuristics; (iii) Humans think and act in different manners as a result of their unique background, including personality and experiences" (Maghsudi & Davy, 2020, pg. 1). To overcome this impediment to widespread IoE adoption researchers have been attempting to create data-driven models that can accurately account for the logical fallacies inherent in human cognition (Maghsudi & Davy, 2020). Presently, research is being conducted on how human behavior can be accurately predicted in a unique scenario using only periphery data involving people with similar profiles (history, personality) in similar situations (Maghsudi & Davy, 2020). Moreover, there are several different versions of these models that are optimized to

account for specific aspects of human cognition most likely to affect a decision in a given environment (Maghsudi & Davy, 2020).

There is an "Iterative strategic thinking" (Maghsudi & Davy, 2020, pg. 6) model that can consider the anticipated actions of others and can potentially be applied to self-driving cars (Maghsudi & Davy, 2020). Moreover, an "Alternation to best-response" (Maghsudi & Davy, 2020, pg. 6) model can be employed to help counteract the effects of inaccurate decision-making, which can be used to improve the efficiency of a "Smart grid" (Maghsudi & Davy, 2020, pg. 6). Lastly, an "Adjustment to utility function" (Maghsudi & Davy, 2020, pg. 6) takes into account different human motivations "such as loss aversion (prospect theory) or a desire for fairness (social preferences)" (Maghsudi & Davy, 2020, pg. 6). Moreover, this function has the potential to help people of all backgrounds and political leanings understand that IoE-enabled applications such as a "Sharing economy, Crowdsourcing, Wireless energy transfer, Cooperative mining" (Maghsudi & Davy, 2020, pg. 6) will lead to the betterment of humanity. Therefore, for the reasons just examined, the future of IoE-enabled systems will likely have mechanisms in place to compensate for errors made by humans, to maximize their overall effectiveness (Maghsudi & Davy, 2020).

IoE Potential Issues

The coming expansion of The Internet of Everything, despite all of its promise, is not without associated risks. For starters, the very aspect that makes many smart devices attractive, their size, may also be their greatest weakness. IoT devices' stature makes it more difficult to implement proper security features as compactness can sometimes overshadow all other

considerations in the IoT domain, which in turn limits the resources available to implement proper security controls (Liu et al., 2020). To that point, “the current IoE mostly adopts the low cost and simplified access protocols (i.e., NB-IoT, LoWPAN) in order to reduce network cost while it makes the communications be vulnerable to malicious attacks such as eavesdropping and forging” (Liu et al., 2020, pg. 71-72). Additionally, encrypting the data “in transit” (Wills, 2022, chapter 7) from the IoT devices within the sphere of the IoE has been suggested as a solution, however, many IoT devices have limited power supplies, and adding encryption to all data transfers may significantly reduce their per-charge battery life (Liu et al., 2020). Additionally, the technology industry is known to progress at a rapid pace, as a result, pressure on organizations to be first movers can create pressure-filled environments that may be incompatible with taking proper due care when considering the security configuration of novel technologies. Further exacerbating this problem is a lack of universal security standards governing IoT devices (Karie, et al., 2021)

Unfortunately, the security standards used for various other technologies do not align well with the security challenges presented by IoT devices used within the IoE framework (Karie, et al., 2021). Although necessary, presently, there is a “lack of specialized universal approved IoT security standards or security assessment frameworks” (Karie et al., 2021). Moreover, there is significant potential for this issue to worsen as IoT devices connected to The Internet of Everything continue to grow more complex and diverse in nature. Furthermore, as the IoE continues to progress both in terms of the overall number of devices connected to it (IoT) and in the level of sophistication of the applications it enables, securing these devices will present new and difficult challenges. Lastly, “this heterogeneous IoT architecture is new to security professionals, and thus, results in increased security risks. Consequently, any attack in this scenario compromises system security” (Marjani et al., 2017, pg. 5257).

Recommendation

It is my recommendation that my client provides their employees with company-issued devices for all technologies that employees need to perform their assigned duties, to prevent enterprise information systems from coming into contact with personal devices that have been connected to unsecured IoT devices. Additionally, I recommend that my client invests in purchasing a "3 year standard reserved Instance" (Amazon Web Services, n.d.), as a 3 year reserve will save the organization a substantial amount of money on a per-Instance use when compared with the pay-as-you-go pricing (Amazon Web Services, n.d.). Finally, this computing resource will be tasked with performing a dedicated, IoE-enabled, analysis of the company's business processes and operations.

Conclusion

In conclusion, the rise of the Internet of Everything is a natural evolution from the Internet of Things (Maghsudi & Davy, 2020). Moreover, this evolution is defined by ubiquitous connectivity between the "four pillars" (Liu et al., 2020 pg. 67) of the Internet of Everything, which are "people, data, process, and things" (Liu et al., 2020, pg. 67). Furthermore, the expansion of The Internet of Everything is inevitable because of the benefits it can offer humanity both at the societal and individual levels (Liu et al., 2020). Therefore, each entity (person, corporation, or nation) needs to carefully weigh the potential benefits of the IoE, i.e., better insights that lead to an improved quality of life, against its current shortcomings (reliant on unsecured/poorly secured IoT devices, and non-existent security standards) to make an informed decision on how to best leverage the IoE. However, those who can successfully create an IT framework that securely harnesses the information produced by the Internet of Everything will be positioned to benefit immensely.

References

Amazon Web Services. (n.d.). *Amazon EC2 Inf1 Instances*. Amazon Web Services, Inc. Retrieved October 11, 2022, from https://aws.amazon.com/ec2/instance-types/inf1/

Dey, N., Shinde, G., Mahalle, P., & Olesen, H. (2019). *The Internet of Everything: Advances, Challenges and Applications (De Gruyter Series on the Internet of Things)* (Illustrated). De Gruyter. https://eds-s-ebscohost-com.ezproxy.umgc.edu/eds/ebookviewer/ebook/bmxlYmtfXzIyMTU0MjdfX0FO0?sid=1ba4ef39-9af9-46f6-83ed-9d2e0ffc3628@redis&vid=1&format=EB&rid=1

Dhaya, R., Ahanger, T. A., Asha, G. R., Ahmed, E. A., Tripathi, V., Kanthavel, R., & Atiglah, H. K. (2022, May 25). Cloud-Based IoE Enabled an Urban Flooding Surveillance System. *Computational Intelligence and Neuroscience*, *2022*, 1–11. https://doi.org/10.1155/2022/8470496

Evans, D. (2012, November 16). *Internet of Everything: Harnessing an Exponentially More Powerful Internet #IoE [Infographic]*. Cisco Blogs. Retrieved October 8, 2022, from https://blogs.cisco.com/digital/internet-of-everything-harnessing-an-exponentially-more-powerful-internet-ioe-infographic

Gacovski, Z. (2019). *Internet of Things*. http://ezproxy.umgc.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2013945&site=eds-live&scope=site&ebv=EB&ppid=pp_Cover

Hu, Q., Yang, H., Wu, J., Fang, H., & Zhang, L. (2022). Material product life cycle analysis Driven by industrial internet of things. *EURASIP Journal on Wireless Communications & Networking*, *2022*(1), 1-21. https://doi-org.ezproxy.umgc.edu/10.1186/s13638-022-02159-7

Jagatheesaperumal, S. K., Ahmad, K., Al-Fuqaha, A., & Qadir, J. (2022). Advancing Education Through Extended Reality and Internet of Everything Enabled Metaverses: Applications, Challenges, and Open Issues. https://arxiv.org/pdf/2207.01512.pdf

Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE Access*, *9*, 121975–121995. https://doi.org/10.1109/access.2021.3109886

Liu, Y., Dai, H. N., Wang, Q., Shukla, M. K., & Imran, M. (2020, April). Unmanned aerial vehicle for internet of everything: Opportunities and challenges. *Computer Communications*, *155*, 66–83. https://doi.org/10.1016/j.comcom.2020.03.017

Maghsudi, S., & Davy, M. (2020). *Computational Models of Human Decision-Making with Application to the Internet of Everything*. https://doi-org.ezproxy.umgc.edu/10.1109/mwc.001.2000250

Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Abaker Targio Hashem, I., Siddiqa, A., & Yaqoob, I. (2017). Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges. *IEEE Access, 5*, 5247–5261. https://doi.org/10.1109/access.2017.2689040

TEDx Talks. (2021, February 24). *The Internet of Everything | Tom Moran | TEDxNewcastleCollege* [Video]. YouTube. Retrieved October 6, 2022, from https://www.youtube.com/watch?v=K-FhMegdlJo

Wills, M. (2022). *(ISC)2 SSCP Systems Security Certified Practitioner Official Study Guide* (3rd ed.). Sybex.