3-25-2017

The Internet of Things: Current Issues and Future Problems

Robert J. LaBuda
Georgia College & State University, robert.labuda@bobcats.gcsu.edu

Matthew H. Gillespie
Georgia College & State University, matthew.gillespie@bobcats.gcsu.edu

THE INTERNET OF THINGS: SURVEYING SOLUTIONS TO THE CRITICAL SEGMENTS OF INTEROPERABILITY, SECURITY, AND BIG DATA

Robert J. LaBuda
Georgia College & State University
robert.labuda@bobcats.gcsu.edu

Matthew H. Gillespie
Georgia College & State University
matthew.gillespie@bobcats.gcsu.edu

ABSTRACT

The internet of things (IoT) has proliferated in the past few years and is fast becoming an integrated part of daily human life. Problems facing IoT and its continued growth include issues with device interoperability, insufficient security protocols standards and a lack of adequate data processing software able to handle the immense amount of data generated by IoT, also known as Big Data. A middleware layer platform is needed to receive, translate, and transmit information between IoT devices which utilize different protocols. A set of security standards will be necessary to begin securing IoT devices. Fog Computing is a solution to the stresses IoT devices can bring to traditional cloud-based computing and analytics. We believe further research could help shape the future decisions in IoT regarding these three critical segments.

Keywords

Internet of Things, IoT, Interoperability, Big Data, Security

INTRODUCTION

The Internet of Things (IoT) represents the future of data generation, machine connectivity and human-life enrichment. Nawir, Amir, Yaakob and Lynn (2016) describe IoT as having three characteristics. First, it is a comprehensive awareness to get the information by using smart objects and network connectivity. Second, it allows the reliable transmission to maintain the high accuracy and real time of the system. Third, it must incorporate intelligent processing to make the systems function smartly. Like its technological predecessors, IoT facing critical hurdles in its continued development and expansion. While the technology of IoT has expanded unabated in recent years, a lack of device standards threatens to significantly slow progress of growth and capability. In most cases, IoT devices lack interoperability, or the ability to communicate, unless each device utilizes the same protocol. Big Data, affects IoT because the data requires an environment conducive to effective storage, management, scalability, and reliability. Clarifying who owns the data per se also presents as a pertinent, but complicated issue. Privacy and security concerns also require the attention of all parties concerned. No security standards are widely-adopted nor is security a paramount concern of vendors or consumers. IoT has developed so rapidly that security protocols have been sacrificed in the name of convenience. The purpose of this paper is to address three critical segments of IoT by exploring currently proposed solutions and future research opportunities.

INTEROPERABILITY

Device interoperability, or the ability to connect and share data, is arguably the most important and complex issue concerning IoT. Issues that arise around the lack of interoperability with IoT-enabled devices include: The inability to test APIs using common approaches and mechanisms, push and pull information from devices using the same interfaces, secure devices using third-party security software and monitor and manage devices using a common management and monitoring layer (Linthicum 2016). The issue at hand can be divided into two separate domains of communication: software interoperability and communication protocol interoperability.

Software Interoperability

The issue concerning the software-based interoperability is that the application program interface, or API, is being developed independently among device manufacturers with little to no standards for interoperability. There is also no discernable effort to promote non-proprietary cooperation. This lack of cooperation has led to vendors adopting an isolationist's view on design and protocols; which is referred to as an "IoT silo". C. Y., & C. H., (2016) define "IoT silo" as a heterogeneity issue, causing different products to be locked in multiple closed ecosystems, which include proprietary device, gateway, web service, and applications.

There is a possible solution for the software interoperability problem. However, while the solution has been stated, its execution is still in development and remains dependent upon the need for well-defined standards. Standardization is difficult because of the varied requirements of different applications and devices. For such heterogeneous applications, the solution is to have a middleware platform, which will abstract the details of the things for applications (Sethi & Sarangi 2017). Li, Xu, and Zhao (2015) concur that a universally accepted service layer is important for IoT. A practical service layer consists of a minimum set of the common requirements of applications, application programming interfaces (APIs), and protocols supporting required applications and services.

Communication Protocol Interoperability

Ma, Liu, Zhou and Zhao (2016) believe that the most important problem of IoT is networking, i.e., how to interconnect large-scale heterogeneous network elements and exchange data efficiently. Communication protocol interoperability faces the same challenges as software interoperability: a lack of standardization has allowed many different transmission protocols to expand unabated. The leading communication technologies used in the IoT world are IEEE 802.15.4(ZigBee), low power Wi-Fi, 6LoWPAN, RFID, NFC, Sigfox, LoraWAN, and other proprietary protocols for wireless networks (Sethi & Sarangi 2017). While standardization is desired, a network layer with the ability to receive the different transmission protocols and convert them into a universally recognized transmission protocol would solve this problem. One solution being developed involves the use of LED visual light communication or VLC. VLC fetch and receive data from nearby IoT devices. The VLC module would act as a master node-gateway that would be placed near these "things" and relay the data to available networks for data transmission and storage via the cloud. This approach would provide backwards compatibility with concurrent imbedded systems, but more research will be needed if this solution is to progress (Ray 2016).

IoT devices must also be able to be identified uniquely to help preserve the integrity of the data generated by the device. Solutions have been suggested address the communication interoperability issue. While traditional protocols such as IPv4 will not work due to the limited number of unique addresses, IPv6 is considered the best protocol for communication in the IoT domain because of its scalability and stability (Sethi & Sarangi, 2017). IPv6 contains 3.4×1038 unique addresses, compared to 4,294,967,296 addresses available in IPv4. While IPv6 appears to be the front-runner as a solution to identifying a vast number of unique devices, a more simplified solution may be required due to the lack of communications standards. , Ma et al. (2016) argue that a straightforward deployment of IPv6 on sensor nodes is not feasible, mainly due to the incompatibility between IPv6 and two-layer protocols such as IEEE 802.15.4 currently used in sensor networks. This is due to IPv6 requiring support of packet sizes much larger than the largest IEEE 802.15.4 frame size.

A universal unique identifier, or UUID, has also been suggested as a possible solution. Li et al. (2015) believe that UUID is critical to a successful deployment in a huge network like IoT, where the identifiers might refer to names and addresses. A UUID-based DHCPv6 Unique Identifier has shown promise as a potential solution, although complications exist. For instance, devices configured using DUID-UUID must select a UUID that is persistent across system restart and reconfiguration events and that is available to all DHCP protocol agents that may need to identify themselves. A UUID that is part of the system firmware, or managed by the system firmware, satisfies this requirement (Narten & Johnson, 2011).

BIG DATA

There are currently billions of IoT devices that can collect, send, and calculate data. The result of this amount of data being collected is exponential growth. Zaslavsky, Perera & Georgakopoulos (2013) discovered that in 2011, data grew to the amount of 1.8 zettabyte (ZB) and is expected to reach up to 35 ZB in 2020. This exponential growth in big data is largely due to the proliferation of IoT devices. However, this technology is only in its infancy as far as development and further growth should be expected to remain exponentially large. Moreover, access to such data needs to be addressed. One approach to data security relies on role-based access control or RBAC. Sicari, Cappiello, De Pellegrini, et al. (2016) argue that the main advantage of RBAC, in an IoT perspective, is the fact that access rights can be modified dynamically by changing the role assignments. The IoT context requires the introduction of new forms of RBAC-style solutions, especially when considering that IoT data will likely represent streams to be accessed in real-time, rather than being stored in static databases. The addition of such great amounts of data must also be analyzed and scrutinized. French and Shim (2016) note that while additional data sources and information produced through continued connectivity and IoT intuitively seems to be useful, more data does not always result in better information. When the amount of data increases without its quality also increasing, the effects can impede progress from a data analytics perspective. It is especially important not just collect data, but also qualify data. Ma et al (2016) found that it is important to evaluate users' data quality, and get rid of malicious and low-quality data. Moreover, data is transmitted with diverse patterns, which is a big challenge to design adaptive data transmission scheme under varied network connectivity for achieving a good balance between transmission quality and network resource consumption. We will discuss following 3 critical components concerning big data and IoT; data management, data analytics and data ownership.

IoT devices are required to operate in an environment that allows for data management that can handle enormous data generation. Traditional cloud computing data management is typically seen as a centralized method with the use of Extract-Transform-Load (ETL) process, Operation Data Stores (ODS) and Data Warehousing. IoT devices are far from centralized and need to interact with a method that can help transition into the centralized data management. This can be accomplished with Fog Computing. Bonomi (2012) describes "Fog Computing" is a highly-virtualized platform that provides compute, storage, and networking services between end devices and traditional Cloud Computing Data Centers". Fog Computing allows traditional data centers to receive data after going through an ETL process, allowing the data to be migrated for storage.

The addition of Fog Computing to traditional cloud-based computing provides IoT devices the ability to complete onsite analytics. The devices that perform onsite analytics thrive on the edge of the system, gather the required data, perform initial analytics, filtering before being sent to the cloud. IoT devices can be spread across many geospatial locations and this innate ability can help to provide significant analytics for the various industries such as energy, transportation, and farming.

The propagation of big data and IoT now leads to the question of "who owns the data?" Currently, it is dependent upon the contractual relationship between the parties involved. Although most devices connected to the Internet do not communicate with each other, this may not be the case soon. As standards for IoT devices are established, and more of these devices possess the ability to pass around data, determining what rights organizations have regarding the use of another's data becomes increasingly important to accomplish and difficult to distinguish. The ownership of data collected from smart objects must be clearly established. The data owner must be assured that the data will not be used without his/her consent, particularly when the data will be shared. Privacy policies can be one approach to ensuring the privacy of information (Whitmore, Agarwal, & Xu, 2016).

SECURITY

IoT also faces the daunting challenge of securing the devices and the data that is generated. A lack of security and privacy could significantly limit the scope to which IoT enriches of lives. Britton (2016) reports that a "2014 HP study revealed that about 70 percent of IoT devices, including sensors and connected infrastructure have vulnerabilities that could be exploited. Eighty percent of devices failed to require strong passwords, 70 percent of devices did not encrypt communications, 60 percent lacked encryption for software updates and another 60 percent had insecure web interfaces (p. 4)." The challenges facing IoT, regarding security and privacy protection, are summarized as resilience to attacks, data authentication, access control, and client privacy (Li et al. 2015). Nawir et al (2016) concluded that without enumerated of security in IoT, attacks will outweigh any of their intended benefits. There are several types of attacks on IoT such as Spoofing/Altering/Replay Routing attack, Denial of Service (DoS) attack, Sybil attack, and node capture attack in IoT.

The extent of the security issue was not completely realized until Eireann Leverett, a researcher in the Centre for Risk Studies at the University of Cambridge, U.K., used Shodan, a search engine for internet-connected devices, to identify more than 100,000 vulnerable IoT devices in 2011, concluding these flaws left them vulnerable to attack by "malicious actors" (Wright, 2017). Not only were IoT devices vulnerable, but flaws were also discovered in nuclear power plant infrastructure, water treatment plants, electric power companies and oil rigs. While many devices have currently forgone robust security protocols, Britton (2016) explains that some of the connected devices may lack the capability of utilizing strong encryption because of a lack of necessary computing and battery power. Cost has also been cited as a reason for lacking security. However, Li et al. (2015) cite a low-cost symmetric-key cryptography algorithms, such as Tiny Encryption Algorithm (TEA) and Advance Encryption Standard (AES), as a proposed solution to protect data exchange.

Developing industry-wide standards will be crucial in confronting security flaws in IoT. Cooperation will also be key when it comes to solving the IoT security problem. Li et al. (2015) believe that "while many organizations are working on the primary standards for IoT, a global collaboration between standards bodies is necessary to deal with the lack of consistency among standards bodies and the standards; the World Standards Cooperation (WSC) should be able to manage the relationships between the international standards bodies and regional standards bodies (p.245)."Although security will need to be addressed by standards committees and vendors, the consumer and the government must also play a role in this process by demanding better protection from threats and breaches. As with policy regarding the internet in the 1990's, the US government has taken a passive role in regulating IoT. However, as IoT becomes more sophisticated, enforcement of a minimum-level security protocol will become a necessity rather than a design choice, especially in regards to consumer privacy. Another solution to data and privacy concerns is using the existing encryption technology used in WSNs being extended and deployed in IoT. However, it may increase the complexity of IoT. The existing network security technologies can provide a basis for privacy and security in IoT, but more work still needs to be done (Li et al. 2015).

FURTHER RESEARCH

We believe that further research into these topics could help provide additional guidance in the selection of a more permanent solution to the current ailments of IoT. Sicari et al (2016) found no literature contributions proposing an architecture able to manage security, privacy and data quality aspects in the IoT environment. Furthermore, Whitmore et al. (2016) found several hurdles stifling further progress:

- The IoT is not well represented in the management literature.
- IoT standards and research are dominated by work done or disseminated in Europe and Asia.
- The IoT literature is dominated by research relating to IoT technology.
- The coverage of IoT driven business models is scant.
- Little work has been done on issues related to the legal and governance frameworks that will regulate the IoT.

Research into the device communication protocols could help narrow the list of commercially-recommended standards, which in turn could help decrease the complexity of the proposed middleware solution. We believe that further theoretical research is necessary in determining the capability of the Fog Computing environment as a viable solution to the management of the immense amount of data that is expected to be generated in the future. If theoretical models support Fog Computing as a capable candidate for managing future data demands, stress-testing in a virtual environment could help determine whether this computing methodology could handle future data growth. Further investigation into the security solutions that IoT devices are employing could help bring about a minimum standard of security. While a robust security suite may not be appropriate for every interconnected device, a standard must be established to quell the data integrity and privacy problems that currently exist.

IoT Issue	Issue Explanation	Proposed Solution	Works Cited
IoT Device Interoperability -	IoT devices lack standards for communication and identification. These devices cannot effectively communicate with each other.	A middleware platform or solution with the capability of receiving, translating, and transmitting communications.	Li, S., Xu, L., & Zhao, S. (2015). Narten, T., & Johnson, J. B. (2011). Ray, P. P. (2016). Sethi, P., & Sarangi, S. R. (2017). C. Y., H., & C. H., W. (2016). Ma, Liu, Zhou and Zhao (2016).
Big Data -	IoT devices produce vast amounts of big data and require special attention to following areas; data management, data analytics, and data ownership.	Utilizing fog computing to manage data and analytics at the local level instead of traditional cloud-based computing.	Bonomi, F., Milito, R., Jiang, Z., & Addepalli, S. (2012). Zaslavsky, Perera & Georgakopoulos (2013). (Whitmore, Agarwal, & Xu, 2016).
IoT Device security -	Security standards for IoT are nonexistent. This places data security and user privacy at risk.	Standards must be established and security must become more of a priority in the design of IoT. Consumers and government must become stakeholders in this process.	Delgado, E. (2015). Britton, K. (2016). Wright, A. (2017). Nawir, Amir, Yaakob and Lynn (2016).

Table 1. Issues and Solutions Concerning the Internet of Things.

REFERENCES

1. Bonomi, F., Milito, R., Jiang, Z., & Addepalli, S. (2012). Fog computing and its role in the internet of things. *Applications, Technologies, Architectures & Protocols For Computer Communication*, 13. doi:10.1145/2342509.2342513
2. Britton, K. (2016). Privacy And Security In The Internet Of Things. *Journal Of Internet Law*, 19(10), 3
3. Huang, C. Y., & Wu, C. H. (2016). Design And Implement An Interoperable Internet Of Things Application Based On An Extended OGC Sensorthings API Standard. *International Archives of the Photogrammetry, Remote Sensing & Spatial Information Sciences, 41*.
4. French, Aaron M. and Shim, J. P. (2016) "The Digital Revolution: Internet of Things, 5G, and Beyond," *Communications of the Association for Information Systems*: Vol. 38 , Article 40. Available at: http://aisel.aisnet.org/cais/vol38/iss1/40
5. Delgado, E. (2015). *The Internet of Things: Emergence, Perspectives, Privacy and Security Issues*. New York: Nova Science Publishers, Inc.
6. Li, S., Xu, L., & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, 17(2), 243-259. doi:10.1007/s10796-014-9492-7
7. Linthicum, David, "IoT Interoperability: An Internet of Broken Things" (2016). Retrieved from https://www.rtinsights.com/iot-interoperability-linthicum/
8. H. Ma, L. Liu, A. Zhou and D. Zhao, "On Networking of Internet of Things: Explorations and Challenges," in *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 441-452, Aug. 2016.doi: 10.1109/JIOT.2015.2493082
9. Narten, T., & Johnson, J. B. (2011). Definition of the UUID-Based DHCPv6 Unique Identifier (DUID-UUID).
10. M. Nawir, A. Amir, N. Yaakob and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks," 2016 3rd International Conference on Electronic Design (ICED), Phuket, Thailand, 2016, pp. 321-326.doi: 10.1109/ICED.2016.7804660
11. Ray, P. P. (2016). Communicating through visible light: internet of things perspective. Current Science (00113891), 111(12), 1903-1905.
12. Rose, K., Eldridge, S., Chapin, L. "The Internet Of Things: An Overview" (2015). Retrieved from http://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf
13. Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal Of Electrical & Computer Engineering*, 1-25. doi:10.1155/2017/9324035
14. Sicari, S., Cappiello, C., De Pellegrini, F. et al. A security-and quality-aware system architecture for Internet of Things. *Information Systems Frontiers* (2016) 18: 665. doi:10.1007/s10796-014-9538-x
15. Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The internet of things--A survey of topics and trends. *Information Systems Frontiers*, 17(2), 261-274. doi:http://dx.doi.org/10.1007/s10796-014-9489-2
16. Wright, A. (2017). Mapping the Internet of Things. *Communications Of The ACM*, 60(1), 16-18. doi:10.1145/3014392
17. Zaslavsky, A., Perera, C., Georgakopoulos, D. (2013) "Sensing as a Service and Big Data". Retrieved from https://arxiv.org/ftp/arxiv/papers/1301/1301.0159.pdf