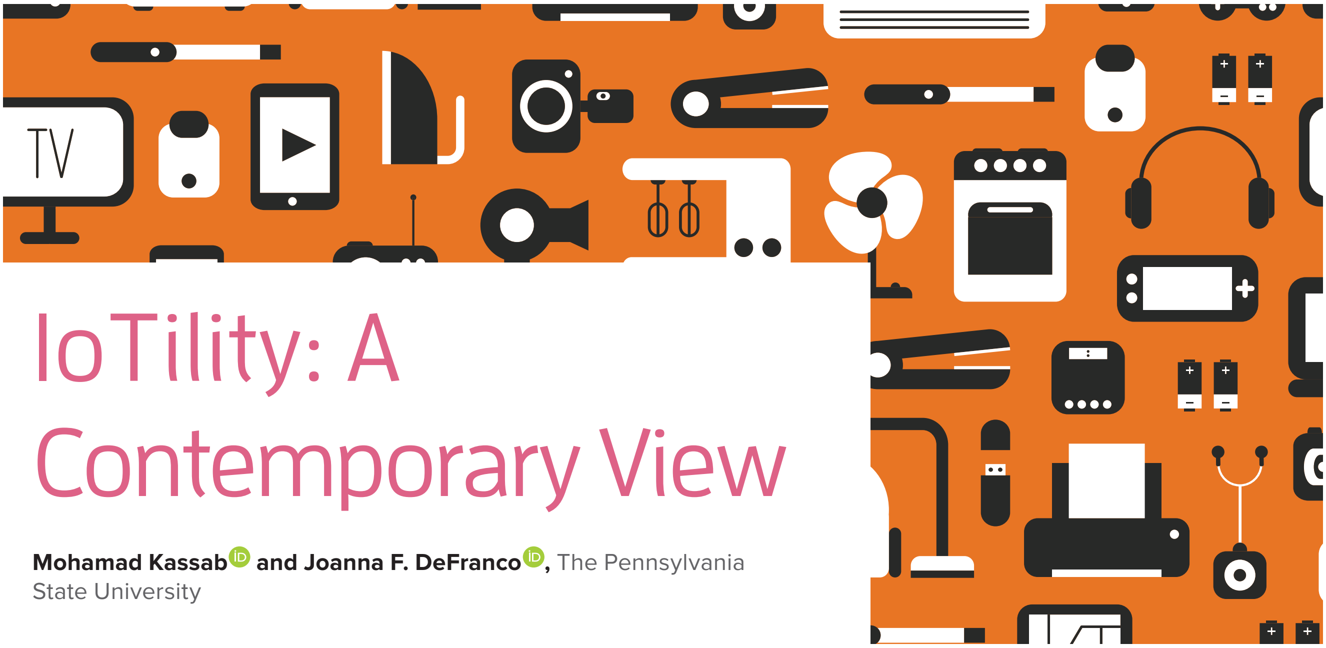

IoTility: A Contemporary View

Mohamad Kassab and **Joanna F. DeFranco**, The Pennsylvania State University

With the increasing ubiquity of the Internet of Things (IoT), some issues with satisfying quality requirements are emerging. This article discusses the current landscape and concerns about IoT quality requirements.

There are various challenges associated with building requirements for Internet of Things (IoT) systems. First, it is a relatively new domain, and capturing requirements based on the proper domain knowledge is necessary before designing and developing IoT-based systems. Second, when specifying the functionality for IoT applications, attention is naturally focused on concerns such as fitness of purpose, wireless interoperability, energy efficiency, and so on.

Conventional requirements-elicitation techniques such as domain analysis, Joint Application Development, and Quality Function Deployment among others are usually adequate for traditional software development requirements. But in some domains, including health care or education, where IoT applications can be deployed, some of the nonfunctional requirements (NFRs) such as security, scalability, reliability, and so on can be of greater concern. In addition, there are new NFRs introduced by IoT systems, such as context awareness and mobility, that traditional requirements-elicitation techniques do not address. Yet there is a scarcity of research on approaches to integrate and evaluate NFRs in IoT applications. We found a few studies that addressed NFRs in IoT system research in general: Mahalank et al.[1] discussed the importance of NFRs in IoT-based smart traffic management systems and pointed out that the success of IoT systems is tightly coupled with the proper analysis of NFRs. Their research highlighted the fact that NFRs are the main drivers for selecting physical components, network protocols, and software integration. In addition, IoT-based NFRs can also interact in the very systems that rely on them. Specifically, attempting to satisfy one requirement can help or hinder the satisfaction of another (that is, increasing security may decrease usability). Other researchers investigated cataloging conflicts among the NFRs found in IoT systems[2] and identifying a model-oriented process to support developers and evaluators in the elicitation, representation, and evaluation of requirements, focusing on NFRs.[3]

In this article, we present the results of a systematic literature review performed to investigate pragmatic concerns when dealing with quality requirements (as well as "ilities") for IoT-based applications. The

Digital Object Identifier 10.1109/MC.2022.3178860
Date of current version: 26 September 2022

EDITOR JOANNA F. DEFRANCO
The Pennsylvania State University; jfd104@psu.edu

following is a panoramic view of the most commonly discussed qualities and their associated concerns for IoT-based applications.

IOT SECURITY

A 2020 survey by Forrester Research[4] reported that the majority of enterprises in North America struggle to identify, monitor, and secure IoT devices in their business. The report also stated that 67% of surveyed businesses are experiencing security incidents related to IoT devices. A second report by Forescout Technologies[5] found that smart buildings, medical devices, networking equipment, and voice over Internet Protocol (IP) phones represent the riskiest IoT device groups, while six of the top-10 IoT device types with the most risk fall into the categories of medical devices and networking equipment. Security has been the most discussed NFR for IoT-based systems. IoT security research revolves around the following security concerns:

1. Sensors' vulnerabilities:
   - *Design vulnerability*: refers to the weaknesses that result from a failure to include proper security measures when developing the device; for example, lacking an intuitive user interface (UI) to change credentials, control interfaces with no user authentication, hard-coded passwords, use of communication protocols that send passwords and other sensitive information in the clear, and allowing for unauthenticated remote firmware updates.
   - *Implementation vulnerability*: occurs when coding errors result in a weakness that can be exploited during a cyberattack; for instance, buffer overflow and improperly seeding random number generators, resulting in security keys that are easy to guess.
   - *Deployment vulnerability*: relates to issues introduced by the user during installation or operation of sensors; for example, using weak passwords, not changing default passwords, not enabling security features, and deploying counterfeit sensors.

Adherence to software development processes that integrate security development help remedy design and implementation vulnerabilities. Examples of these processes are the Open Web Application Security Project Secure Software Development Lifecycle and Microsoft's Security Development Lifecycle. On the other hand, many practitioners have proposed solutions to the problem of default credentials in IoT systems, ranging from the usual recommendation to change credentials—encouraging manufacturers to randomize passwords per device—issuing Manufacturer Usage Description specifications[6] that allow manufacturers to specify authorized network traffic, to more advanced and strict ideas, like enacting legislation that regulates the operation of IoT devices [for instance, California legislation (Senate Bill-327), which bans default passwords in IoT-connected devices].

2. *Communication channel*: The communication mechanisms will vary by device but may include wireless protocols ranging from Zigbee and Bluetooth Low Energy (BLE), to Wi-Fi, cellular data, and Ethernet. Communication channels are prone to malicious disturbances and interruptions. Although using transport encryption (for example, Wired Equivalent Privacy and Wi-Fi Protected Access 2) should be considered, it may not be sufficient. Zigbee and BLE already have encryption built into the protocol but also have known vulnerabilities. Adopting standards like Transport Layer Security (TLS) or Datagram TLS should also be used when possible.
3. *Aggregators*: These are software implementations based on mathematical function(s) that transform groups of raw data received from IoT devices into intermediate, aggregated data, and then transmit the aggregation result to servers. Although an aggregator shall act as an honest but curious entity whose duty is aggregation and relaying, it may also become a point of attack (for instance, by feeding them fraudulent data or denying them the ability to execute). An adversary may compromise the aggregator to infer the actual data of each connected IoT device, which may compromise the devices' privacy. The existing data-aggregation schemes shall be designed with security in mind so that when an adversary forges or modifies a report, the malicious operations should be detected by an aggregator. Aggregators shall also guarantee that the received data are valid and derived from legal entities.
4. *Upgrade process*: An IoT device's firmware is often subject to receiving feature

and configuration updates. These updates shall be carried through a secure process with which it is ensured that the firmware is coming from a trusted party. Machine-to-machine authentication methods can be used by the IoT device to authenticate the upgrade source before downloading the new firmware image. Cryptographically secure hash validation can also be used to verify the firmware before it is stored on the device. The IoT Firmware Update Architecture,[7] recently proposed to the Internet Engineering Task Force, provides the details needed to implement a secure firmware update architecture, including hard rules defining how device manufacturers should operate.

Machine-to-machine authentication methods can be used by the IoT device to authenticate the upgrade source before downloading the new firmware image.

IOT SCALABILITY

Scaling an IoT deployment and infrastructure can be a challenging endeavor. A comprehensive scalability strategy for IoT-based applications shall address the following concerns:

- *Wireless capacity*: Connected devices may generate a deluge of data traffic, which imposes great bandwidth challenges. It is essential to assess whether the wireless system can accommodate the fast-growing number of endpoints that arrive down the line. Metrics such as the number of messages that can be handled per gateway per day can help evaluate the scalability of a wireless network. In addition, with subgigahertz wireless technology, it is possible to segregate IoT networks from other 2.4-GHz legacy systems to mitigate congestion issues.
- *Network architecture*: The short radio range of many wireless protocols dictates the necessity to distribute IoT devices and repeaters delicately. Adding or moving nodes can lead to unpredictable performance or troubleshooting challenges. A star topology structure can help in this direction. On the other hand, although the cloud is on the radar to handle massive IoT data streams, a combination with on-premise infrastructure is often called into action to satisfy a balance between cost, performance, security, and scalability. The hybrid workflows and data migration from edge to cloud shall be carefully assessed for scalability in this case. Containerized-based design and microservices make a good fit with hybrid architecture due to their platform-agnostic nature and the possibility of leveraging container-orchestration tools like Kubernetes to easily deploy, manage, and scale the software to adapt to changing needs.
- *Data storage*: By embedding sensors into front-field environments as well as terminal devices, an IoT network can collect rich sensor data that reflect real-time environment conditions of the front field and the events/activities that are occurring. Because the data are collected in the granularity of an elementary event level in a 7 × 24 mode, the data volume is very high, and the data-access pattern also differs considerably from traditional business data. This has motivated a new generation of data management solutions; for example, the NoSQL database, map-reduce distributed computing framework, and so forth.

INTEROPERABILITY FOR THE IOT

Interoperability is key to unlocking all of the IoT paradigm's potential, including immense technological, economic, and social benefits. Interoperability is a top challenge, possibly preventing the IoT from reaching its full potential. The interoperability challenge can manifest itself in several ways: lack of a reference standard, vast heterogeneity of IoT systems, and limited connectivity among different transport protocols such as Ethernet, Wi-Fi, and Zigbee cause an inability to complement and integrate collected data from different IoT devices.

Nevertheless, McKinsey Co. estimates that resolving these interoperability issues can unlock more than US$4 trillion per year in potential economic impact from IoT use by 2025.[8] It is essential to consider that IoT deployments have specific interoperability needs:

- *Technical*: ability to use a physical communications infrastructure to transport data.
- *Syntactic*: ability to share syntax or common information model structures for data and establish a protocol to share the information as specific typed data.
- *Semantic*: ability to establish data meaning.

Today, industry is beginning to coalesce around the notion that devices should simply work together in a plug-and-play fashion, and technology standards are progressively becoming popular to foster horizontal interoperability. The Standard for IoT Messaging, for example, is an open source networking protocol that transports messages between devices and has been serving as a lingua franca for the wide range of IoT components that can use it to exchange information.

IOT PERFORMANCE

As with any network technology, responsiveness and speed are essential for reliable IoT network operation. The following several factors can affect the performance of IoT systems:

- massive numbers of connected devices to the networks
- limited bandwidth
- network topology
- limited storage and data-utilization capacity
- malfunctioning devices.

Edge computing can help with utilizing network bandwidth because it forces most bandwidth-hogging processes to run directly on IoT devices, reducing the need to send data back and forth to centralized servers for processing. Although traditional wide area network (WAN) links often lack the network intelligence necessary to move IoT data across the network in the most optimal manner, utilizing a software-defined WAN (SD-WAN) can improve IoT network performance by combining two or more WAN links with artificial intelligence, allowing data to travel over the optimal path toward its final destination. Network segmentation and adaptive contention window are two other performance tactics for IoT-based applications.

IOT USABILITY

Despite the enthusiasm of early adopters of the IoT, approximately only 25% of IoT projects succeed.[9] Although early adopters worry about interoperability, late adopters are more concerned with IoT usability caused by the complexity and availability of IoT expertise to be able to connect, set up, and navigate through the IoT system. Thus, usability design is a particular challenge with the IoT. First, given the wide range of device types, achieving consistency among the various UIs within a connected IoT network is not an easy task. Second, many consumers do not understand that IoT devices, when not properly secured, can give hackers access to much more than just that one device, hence the UI shall be designed for easy navigation through IoT security protocols. Third, UI design for IoT applications is often constrained by limited display size, functionality, asynchronous operation imposed by device processing and battery limitations, or limited ability to control (for instance, UIs for smart home devices are often limited to a small set of onboard features, while a broader set of control parameters are only accessible remotely via a mobile device).

On top of this, users will often invent a use for the device that was not a part the original market concept, like an IoT-enabled tractor that sends an alert when servicing is required. In this case, a farmer may utilize the feature to also pay employees based on productivity. Establishing various use cases matters because they identify the usability models specific to the device, task, or user.

As with any network technology, responsiveness and speed are essential for reliable IoT network operation.

IOT DISCOVERABILITY

To realize the vision of truly connected things, there must be mechanisms available for automatic discovery of resources, and their properties and capabilities as well as the means to access them. Device discovery is a complex problem for the IoT, but the general problem of discovery within networks has been studied for decades. Broring et al.[10] presented four categories of IoT discovery technologies:

- The discovery of "things" that are in close spatial proximity to a client (<10 cm with near-field communication, <100 m with BLE).
- The discovery of endpoints of "things" on the network (for example, multicast domain name service, Multicast Constrained Application Protocol, Simple Service Discovery Protocol, and Web Services Discovery).
- A central directory is used for the discovery of IoT devices and their resources [for instance, the constrained RESTful (CoRE) Resource Directory, Extensible Messaging and Presence Protocol IoT Discovery, HyperCat, Sensor Instance Registry, and Simple Protocol and RDF Query Language Endpoint].
- Accessing IoT device metadata once they are discovered (for example, CoRE Link Format, Open Geospatial Consortium Sensor Observation Service, and Optical Markers).

Nevertheless, the discoverability of IoT devices can contradict some aspects of security, with some illustrative scenarios discussed in the National Institute of Standards and Technology article on IoT trust concerns.[11]

IOT MOBILITY

Many IoT devices intrinsically work over mobile systems or evolve toward mobility or both because they move with humans, as is the case with smartphones and wearable devices or because they move by themselves, similar to robots. Based on their locations, these devices are likely to change their IP addresses and networks frequently.

Routing protocols such as Routing Protocol for Low-Power and Lossy Networks must reconstruct a tree-like routing topology called the *destination-oriented directed acyclic graph* each time a node goes off the network or joins the network, which adds substantial overhead to the system. Fortunately, the research community has been active in developing algorithms to address the attributes of IP mobility management within Ipv4 and Ipv6.

OTHER "ILITIES"

Deploying IoT systems opens the doors for new quality attributes to emerge. There are questions about the morality that the IoT may play in human lives, particularly concerning personal control. Applications in the IoT involve more than computers interacting with other computers. Fundamentally, the success of the IoT will depend less on how far the technologies are connected and more on addressing new emerging qualities, such as humanization (or dehumanization), that are particular to the domain of deployment.[13] When constructing IoT systems for the health-care domain, for instance, it is important to engage all stakeholders when trying to define a notion of "caring" for a new health-care system. The emerging "caring" quality in the context of IoT systems was discussed by Laplante et al.[12]

IoT technology may also reduce people's autonomy, move them toward particular habits, and then shift power to corporations focused on financial gain. When deploying the IoT in the education domain, for example, this effectively means that controlling agents can become the organizations that regulate the tools used by academic professionals but not the academic professionals themselves.

In summary, quality requirements have always been a challenge to the development community. This challenge only becomes greater with the introduction of new IoT "ilties" and their interaction with each other. C

REFERENCES

1. S. N. Mahalank, K. B. Malagund, and R. Banakar, "Non-functional requirement analysis in IoT based smart traffic management system," in *Proc. Int. Conf. Comput. Commun. Control Automat. (ICCUBEA)*, 2016, pp. 1–6, doi: 10.1109/ICCUBEA.2016.7860147.
2. R. M. Carvalho, R. M. Andrade, and K. M. De Oliveira, "Towards a catalog of conflicts for HCI quality characteristics in UbiComp and IoT applications: Process and first results," in *Proc. 12th Int. Conf. Res. Challenges Inf. Sci. (RCIS)*, 2018, pp. 1–6, doi: 10.1109/RCIS.2018.8406651.
3. T. Ruiz-López, M. Noguera, M. J. Rodríguez Fórtiz, and J. L. Garrido, "Requirements systematization through pattern application in ubiquitous systems," in *Ambient Intelligence-Software and Applications*. Berlin, Germany: Springer-Verlag, 2013, pp. 17–24.
4. "State of enterprise IoT security in North America: Unmanaged and unsecured," Forrester Research, Cambridge, MA, USA, 2020. https://bit. ly/38D17Tg
5. "The enterprise of things security report: The state of IoT security," Fourscout, San Jose, CA, USA, 2020. https://bit.ly/ 3MIpaPy
6. E. Lear, R. Droms, and D. Romascanu, "Manufacturer usage description specification," Internet Engineering Task Force, Tech. Rep. RFC 8520, Aug. 5, 2019.
7. B. Moran, M. Meriac, H. Tschofenig, and D. Brown, "A firmware update architecture for Internet of Things devices," Internet Engineering Task Force, Internet-Draft, 2019. https://www.ietf.org/archive/id/draft-ietf-suit-architecture-02.txt
8. J. Manyika *et al.*, "Unlocking the potential of the Internet of Things," McKinsey Global Inst., Jun. 1, 2015. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world
9. "Cisco survey reveals close to three-fourths of IoT projects are failing," Cisco Press Release, 2017. https://bit.ly/3wxjn8O (Accessed: May 15, 2022).
10. A. Broring, S. K. Datta, and C. Bonnet, "A categorization of discovery technologies for the Internet of Things," in *Proc. 6th Int. Conf. Internet Things*, 2016, pp. 131–139, doi: 10.1145/2991561.2991570.
11. J. Voas, R. Kuhn, P. Laplante, and S. Applebaum, "Internet of Things (IoT) trust concerns," NIST Cybersecurity White Paper, vol. 1, pp. 1–50, Oct. 17, 2018. [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/white-paper/2018/10/17/iot-trust-concerns/draft/documents/iot-trust-concerns-draft.pdf
12. A. Laplante, M. Kassab, N. L. Laplante, and J. M. Voas, "Building caring healthcare systems in the internet of things," *IEEE Syst. J.*, vol. 12, no. 3, pp. 3030–3037, 2017, doi: 10.1109/JSYST.2017.2662602.
13. M. Kassab, J. DeFranco, and P. Laplante, "A systematic literature review on internet of things in education: Benefits and challenges," *J. Comput. Assisted Learn.*, vol. 36, no. 2, pp. 115–127, 2020, doi: 10.1111/jcal.12383.

MOHAMAD KASSAB is an associate research professor of software engineering at The Pennsylvania State University, Malvern, Pennsylvania, 19355, USA. Contact him at muk36@psu.edu.

JOANNA F. DEFRANCO is an associate professor of software engineering at The Pennsylvania State University, Malvern, Pennsylvania, 19355, USA. Contact her at jfd104@psu.edu.