Published in final edited form as:

IEEE Internet Things J. 2019 ; 6: . doi:10.1109/JIOT.2019.2911010.

Replication of Smart-City, Internet of Things Assets in a Municipal Deployment

Alexander Nelson [Member, IEEE],

Department of Computer Science and Computer Engineering, University of Arkansas,
Fayetteville, AR, 72701 USA

Greg Toth [Member, IEEE],

IoT Dev Labs Inc., Tysons Corner, Virginia, USA

Dennis Linders,

Montgomery County, MD, Rockville, Maryland, USA

Cuong Nguyen,

National Institute of Standards and Technology, U.S. Department of Commerce, 100 Bureau
Drive, Gaithersburg, MD, USA.

Sokwoo Rhee

National Institute of Standards and Technology, U.S. Department of Commerce, 100 Bureau
Drive, Gaithersburg, MD, USA

Abstract

Recent efforts to integrate Internet Of Things (IoT) technologies into Smart City constructs have proven successful through proof-of-concept deployments in multiple cities. To facilitate additional deployments, standardization and dissemination of best practices for these technologies is critical. To that effort, this work seeks to establish a framework in a set of IoT hardware, software, and wireless radio components that are flexible to address several use cases and easily replicable to new deployments. Moreover, the framework aims to be standards-based and to use best practices for cybersecurity to maintain security and privacy. The framework is developed, deployed, and tested through three sub-projects in different domains and a live testbed housed by a municipal government, collecting over 160 million distinct sensor records from eight physical locations over a period of 8 months. Additionally, the framework is replicated to a separate jurisdiction to prove ease of replicability. This work identifies common barriers to IoT adoption and replication, both technological and organizational, and enumerates the approaches that were taken to overcome those barriers in these projects.

<http://www.alexanderhnelson.com>.

Disclaimer

Official contribution of the United States government; not subject to copyright in the United States. Certain commercial products may be identified in order to adequately specify the procedure; this does not imply endorsement or recommendation by NIST, nor does it imply that such products are necessarily the best available for the purpose.

Keywords

Smart City; Internet of Things; Replication; Environmental Sensing

I. Introduction

THE application of Internet of Things (IoT) technologies to the public space has become an important and very impactful area of research. Smart city is the concept of using sensing and data collection in municipal environments, and incorporates many IoT technologies. Many cities, communities, and municipal governments are looking to smart city technology as the next evolution of e-governance, enabling new interactions with the public or reducing overhead of existing policies. Municipal governments are also striving to take advantage of the advances of Information and Communication Technology, but specific implementation of the Smart City technology is often slowed down by the lack of generally-accepted best practices and broadly-deployed standard-based solutions, as well as by the necessary due processes for procurement and long budget cycles.

The market and technology landscapes for IoT solutions are highly fragmented because of the complex and diverse nature of the problems they are trying to address. The lack of consensus on priorities among municipal governments exacerbates system fragmentation. This fragmentation is one of the fundamental reasons why we only see the incremental growth of the IoT and smart city deployments instead of the exponential growth, which has been longed for in the market.

To alleviate the issue of fragmentation in the IoT and smart city market, it is essential to create a momentum for convergence both from the market and technology perspectives. The momentum of convergence can be best accomplished by voluntary cooperation and collaboration among relevant stakeholders. In order to encourage cooperation and coordination among stakeholders – cities, communities, companies, academic institutions, and nonprofit organizations – the National Institute of Standards and Technology (NIST), a bureau of U.S. Department of Commerce, have worked on two projects to facilitate collaboration among stakeholders [1]. NIST's smart-city convergence efforts began with the Smart America Challenge program, held with the support of the Office of Science and Technology Policy (OSTP) Presidential Innovation Fellows program at the end of 2013 [2], [3]. This effort became the genesis of the NIST Global City Teams Challenge (GCTC) [4] which was designed to accelerate market-driven consensus. Acceleration was expected to occur because the GCTC would provide a platform for cities/communities and technology providers to collaborate and demonstrate replicability, scalability, and sustainability of the smart city and IoT projects. The goal of the GCTC was to identify best practices that can be shared among stakeholders instead of falling in the vicious cycle of "reinventing the wheel."

To achieve this goal and accelerate the technology-driven consensus, NIST has worked on the Internet of Things Enabled Smart City Framework [5], which applied the concept of Pivotal Points of interoperability (PPI) to the technology components of well-known IoT and smart city technologies to analyze and understand the most probable path to interoperability. These works were consistent with NIST's technology strategy, which involved using systems

engineering principles (NIST's Cyber-Physical Systems Framework [6]) to work bottom-up from device-level performance characterization to system performance.

The analysis of PPI enables smart cities to replicate their technologies between disparate instances and localities. Replication of systems is important to reduce the overhead cost of introducing new technology. This replication must occur at several levels: between geographically distributed cities, between organizations operating within the same city, and even between logical divisions within the same organization. Cloud-based infrastructure and code containerization can facilitate some of this behavior, but IoT and cyber-physical systems inherently have a physical footprint that brings in complications. For example, municipalities may have exclusive deals with vendors, specific pieces of hardware may not be available in some regions, or hardware may be obsolete before a later city can do the same implementation. These examples demonstrate how hardware heterogeneity between iterations can be introduced even with intentions to perform the same tasks. Heterogeneous deployments create additional complexity and can adversely affect performance of systems [7]. Moore's law has historically guaranteed that hardware becomes obsolete quickly, and even cloud providers have heterogeneous hardware for the same type of cloud instances [8].

II. Motivation

Our project sought to answer a key question: How do we make it easier and more efficient to replicate Smart-City solutions from one city to another? We decided to conduct the research needed to answer this question in a real-world setting. The primary motivation for this decision is quite simple. The complexities and messiness of living, breathing cities and communities cannot possibly be replicated in the controlled environment of an academic lab. So, in our view, the cities, themselves, must become the lab for experimentation with Smart-City technologies.

In addition to being built in a real world, there are a few necessary conditions for replicability beyond the bounds of a single organization. First, such a technology must be built with high standards for security and privacy. Many municipal operations can be safety critical and the introduction of additional wireless sensing and actuating nodes can provide additional vectors for an attacker to target. Similarly, privacy becomes a more daunting issue with pervasive sensing. Personally Identifiable Information (PII) or other sensitive information can unintentionally be collected as a consequence of the sensing paradigm. For instance, a network of high-resolution traffic cameras may capture face images, license plate numbers, and place of residence of a person in real-time. It is of great importance to consider privacy and security implications throughout the ideation, creation, and iteration of systems – rather than as an afterthought – to prevent breaches that could cause harm and undermine public trust in municipal systems.

Second, for an IoT architecture to be replicable across logical boundaries, it must be flexible to the computing environment. Government organizations will have different contracts, vendors, suppliers, and organizational rules that prevent carbon-copy adoption of an existing system. To facilitate these environmental differences, the architecture should (whenever possible and subject to verification of privacy and security) adopt the following three

conventions: 1) be vendor and technology agnostic, 2) implementable in cloud, on-site, or hybrid deployments, and 3) leverage open-source software.

The first two conventions allow for the architecture to conform to existing agreements and policies for ICT in government organizations. The use of open source software has advantages in that the software can be the same across instances, is free to adopt, and is less subject to becoming obsolete since the source code can be updated. However, open source developers are rarely proficient in current privacy and security practices, and thus the open source software should be verified and trusted, or quarantined and firewalled to prevent unauthorized access.

Finally, data exchange should be managed through a set of standards-based, secure, and replicable technologies. Certain antiquated data-exchange protocols may be required based on legacy software, but those should be bridged into secure and reliable protocols at the ingress point. Application containerization (like Docker and Kubernetes) and micro services facilitate vendor/supplier agnosticism as the virtual machine structure abstracts the underlying differences in hardware and operating system. Data should be managed in formats that are appropriate and descriptive. Moreover, this data should be readily available for recall or deletion in order to scale or modify technologies and vendors after initial deployment.

III. Methodology and Application

The project's real-world implementation was based on the "learning by doing" methodology developed by the Innovation Action Research (IAR) group [9]. We applied IAR's methodology to the Smart-City architecture problem discussed above. Our four-step process – drawing inspiration from IAR's and Kaplan's research methodology [10] – is collaborative and iterative (see Figure 1), and starts by first observing the local implementation and by learning from peers and industry partners. The results of those process are used to determine what, if any, barriers are preventing a successful implementation.

The team next develops techniques and assets ranging from adopting standards to articulating common guiding principles to overcome these barriers. Next, the team validates and refines techniques and assets based on experience in practice and the resulting lessons learned. Lastly, the team concludes with a dissemination stage with a focus on 1) communicating the findings, 2) collaborating on improvements, and 3) promoting replication in other jurisdictions. Importantly, this process focuses not just on technical challenges and solutions but also on the institutional, political, and business considerations underpinning impactful and replicable Smart-City implementations. Our implementation of this research methodology has been applied to several Smart-City-encountered challenges. One of the major challenges we found in our project is the inherent difficulty in replicating hardware solutions across any multi-dimensional, real-world organization. Creating IoT technologies that work well in the laboratory or a pilot test environment is still a mostly manual process. The engineers and technologists executing that manual process typically work very closely together with the development and deployment teams. Their principal

responsibility is to fix technical issues once a technology leaves the pilot phase and is ready to be integrated into the existing real-world infrastructures.

Significant challenges, however, remain in discovering those fixes. These challenges were identified and examined 1) as part of the authors work implementing a replicable Smart-City pilot program and 2) through discussions with the broader Smart-City community and peers. In this section, we identify four “barriers” to replication that we uncovered as part of this project. In Table I, each of the four barriers are categorized by the type of considerations and organizational units that are affected.

Barrier 1 – Matching IoT Solutions to Use Cases

The first barrier involves the first question most organizations will ask, “Why should we use IoT in our organization?” In many cases, this question can be answered by saying that IoT solutions can improve both the performance and the use of existing technologies. Use cases abound where IoT has been deployed effectively either 1) to reduce the overhead of existing services or 2) to provide better service to constituents. Regardless, many municipal organizations are hesitant to implement similar solutions for several reasons. We enumerate a few here:

1. The technology exists, but municipalities are unaware of that technology.
2. The technology exists, but is not yet mature.
3. The technology exists, but the return on investment is unclear.
4. The technology exists, but does not interface well with existing infrastructure.
5. The technology exists, but it is not clear whether it is suitable in the local context and environment or how it can be appropriately tailored.

Any of these five questions if not properly answered can derail a project. However, the answer to these questions can often be found in peer organizations that have performed similar works. While our project focused on finding answers to some of these questions, a replicable architecture can provide a basis on which reasonable estimates can be inferred by future implementations.

Barrier 2 – “Not Invented Here” Syndrome

The second barrier that is often encountered is the tendency for organizations to be inherently distrustful of systems not developed internally the so called the “Not Invented Here” (NIH) syndrome [11]. This syndrome, unfortunately, has been credited with the degradation of performance within IT and R&D structures [11]. In the teams experience, there are two major reasons for such a degradation. First, there is a tendency to focus both on the near-term and maintaining the current, existing infrastructure. Second, there is a fear that external solutions would limit access to data or violate existing data-privacy structures.

The negative impacts of the NIH syndrome can be significant, because key stakeholders frequently make decisions backed only by their experience and knowledge of the past. For instance, newer, open-source, IoT solutions offer a highly promising avenue for promoting Smart-City replication. Moreover, these solutions must often be integrated into a highly

complex, existing IT infrastructure that may contain a combination of home-grown and vendor solutions, varying computing environments, tools, languages, protocols, and data formats governed by longstanding, but at times outdated, IT governance processes. Injecting such open-source, IoT solutions, which often lack service-level agreements and other assurances of reliability and sustainability, into such an environment substantially increases the integration challenge. That increase places tremendous constraints on replicating a successful, Smart-City solution from one jurisdiction to another. Hence, traditional IT organizations, who follow the NIH paradigm, don't use open-source solutions.

Smart-City implementations face further integration challenges because the chosen IoT solutions need to integrate not only with the jurisdiction's IT infrastructure but also with each jurisdiction's unique policies, organizational structures, terrain, weather, boundaries/size, and strategic goals.

Barrier 3 – Communication and Collaboration across inter- and intra-organizational boundaries

The third barrier is encountered as the organization attempts to deploy and integrate IoT solutions. This barrier arises for two major reasons. First, there is apprehension to discuss technological approaches between organizations or even between divisions within an organization. Second, there is a general lack of awareness of what others have done or plan to do. As a result, organizations are often unaware of duplication and mistakes that may have already been solved elsewhere.

Barrier 4 – Cybersecurity awareness and apprehension

The fourth barrier relates to the role of cybersecurity. When new technologies are being piloted, there is often a tendency to focus on functionality and time-to-market and leave robust security toward the end. This tendency can lead to insecure components being connected to mission-critical enterprise environments. This situation can easily introduce new cybersecurity risks to that environment – risks that may not be well understood. On the other hand, some vendors focus on complex and comprehensive cybersecurity at the beginning. This emphasis on security at an early stage of the project can sometimes limit the ability to validate the utility and business value of a candidate solution – even if it happens to be highly secure.

IV. Implementation

The community selected for this project provided a highly conducive environment for this work. First, the community offered scale, with a single government entity covering 500 square miles and 1 million residents. Second, it had diversity, with over 50 distinct places in a mix of urban, suburban, and rural settings. Third, the community offered important enablers by hosting 1) a number of prominent, federal-research centers active in the Smart-City space and 2) a home-grown, locally operated makerspace – the “Thingstitute” – that provides a collaborative, Smart-City testbed and ecosystem. That ecosystem includes local governments, corporate partners, academic researchers, and the public at large. The

Thingststitute ensured that the project was led and coordinated by the local government rather than by the private sector or academia.

The research was conducted through linked sub-projects in three disparate domains: 1) Unmanaged aging-in-place, 2) municipal-provided transportation, and 3) environmental monitoring. The first project is depicted in Figure 2. Sensing devices were given to residents of an independent senior living facility to place in their home environment. The facility, located in Rockville, MD, houses approximately one hundred residents. Sensor boxes were placed in the front office and in three resident's family areas. These residents were compensated through grocer gift cards to offset any power usage and time interacting with the research staff. The sensing devices monitored environmental conditions including temperature, humidity, and CO₂. The sensing devices were composed of off-the-shelf components and single board computers (e.g. Raspberry Pi, Beaglebone Black). Initial sensor devices communicated through a selection of Ethernet, 802.11 Wi-Fi, or a 3G Cellular radio depending on the connectivity of each apartment. Residents were expected to provide their own Internet connectivity, and therefore there was no consistent access method. In addition to the sensor boxes, participants were given emergency pushbutton medallions that could communicate using a low-power wide-area network (LPWAN) radio in the form of an Ultra narrow band (UNB) Sigfox [12] transceiver, with two tower sites positioned in the downtown region of the community. Care was taken to prevent capture of any PII during this phase, including anonymizing any personal data on the server (names, addresses, etc). Later, speech recognition devices (specifically an Amazon Echo) were integrated into the environment with custom hooks into the county services for commands. The sensor data from the devices are transmitted to the cloud instance in real-time through the MQTT broker, then analyzed and combined with voice and emergency button notifications to determine if any intervention action needs to take place. No real emergency conditions were detected during the trial period, but simulated emergencies (e.g. medallion press, dangerous temperature) were tested and detected by the framework.

The second project focused on the municipal transportation agency that operates a fleet of approximately 350 buses. These vehicles communicate through an aged, proprietary radio technology, that has a slow check-in frequency and drops packets quite frequently. As a consequence, the Global Positioning System (GPS) positions that are used for real-time localization are often stale and unusable for public engagement to determine when buses will be arriving at stops. A mobile device with an active GPS antenna 3GPP LTE (3rd Generation Partnership Project Long-Term Evolution) radio chipset was added into vehicles with a 3 second update frequency, resulting in much higher quality real-time positioning. This device also acts as a gateway for introducing additional features such as passenger counting, relaying real-time on-board diagnostics information, and providing municipal, wireless, Internet connectivity. Two device setups were tested during the initial prototyping. First, a Digi International Transport WR44R acted as the cellular backhaul for a single board computer (Raspberry Pi) with a GPS receiver. The WR44R was also being tested for providing publicly accessible Wi-Fi on the bus. This same setup was also tested with a Cradlepoint IBR900 gateway as the backhaul. Second, an application was written in Android Studio for a MachFu MACHGateway to send GPS information through MQTT directly over

its cellular connection. Both of these systems were able to communicate GPS location to the backend server with higher update rates and fidelity for the downtown regions.

The third project focused on deploying environmental sensors to measure temperature, humidity, barometric pressure, CO, particulates, light and motion in both indoor and outdoor environments. Sensing units were designed and deployed using several forms of communications to allow network data transfers: 1) Wired Local Area Network (LAN), 2) Wireless Wi-Fi and 3) Wireless LoRaWAN [13]. Each sensing unit contains multiple sensors that periodically generate measurement records that are securely transmitted to a data-exchange platform running in a cloud environment. These devices were composed of single board computers with off-the-shelf sensors. The communication was facilitated through on-board Ethernet LAN, an Edimax N150 Wi-Fi adapter, or a LoRaWAN radio chipset (e.g. Adafruit RFM95W). Sensors were placed in different physical locations both indoor and outdoor in Rockville, MD, Tyson's Corner, VA, and Washington D.C.

V. Data Exchange Platform

To facilitate these three very different projects, a flexible and secure communication and data-exchange platform (Figure 3) that supports a set of interaction patterns (Figure 4) is needed for producing and consuming data. MQTT [14] was chosen as the standard for a real-time, publish-subscribe messaging protocol. A commercial cloud environment is used to implement a real-time MQTT data backbone, that provides several key services: 1) Secure MQTT endpoints for connecting devices and applications; 2) Certificate-based credentials for authenticating devices and applications; 3) Security policies and roles for authorizing access to data and resources within the cloud environment; 4) a rules engine for transforming and routing messages in real-time; 5) a variety of data storage, data processing and data analytics services for recording, processing, extracting and analyzing collected data; and 6) the ability to easily scale capacity up or down as needed.

Sensing devices that are directly connected to the Internet via LAN, Wi-Fi or LTE implement integration pattern (Fig. 4a) where the sensing device is a MQTT publisher. An application program runs on the sensing device to control the physical sensors, generate formatted data records, and securely publish data records to the MQTT backbone through the Internet. Once data has been published to the backbone it is transformed, routed and consumed by any number of consuming applications.

Sensing devices connected through LoRaWAN wireless communication have an additional bridging application program that implements pattern (Fig. 4e) to bridge between the LoRaWAN system (using its Application Programming Interface (API)) and the data exchange platform (using MQTT publish pattern (Fig. 4a)). The bridging application reads data from the LoRaWAN server, generates formatted data records, and securely publishes data records to the MQTT backbone. For the bus GPS application, a bridging application implements pattern (Fig. 4e) to bridge between the bus GPS (using its API) and the data-exchange platform (using MQTT publish pattern (Fig. 4a)). Applications that read real-time, bus location, data from the data exchange platform do so as MQTT subscribers using MQTT subscribe pattern (Fig. 4a).

Once data arrives in the data backbone it is processed and routed based on the MQTT topic. Topics within the data exchange platform operate as categories representing different data models. Using a JSON-based MQTT payload enables extensible data models, including the use of a standard ontology or a proprietary municipal data model. Using these categories, the data is processed in real-time by: 1) Raw data is recorded in log files; 2) Raw data records are transformed into usable data records by adding or removing selected fields; 3) Certain data records (e.g. from specific sensor units) are republished to auxiliary MQTT topics; 4) Data is periodically extracted and downloaded for offline data analysis; 5) Data is fed into cloud-based analytics services for viewing within the cloud environment; 6) A real-time dashboard application (written in open source Node-RED [15]) connects to the backbone as a MQTT subscriber (pattern Fig. 4a)) and displays real-time readings from the sensing units; and 7) Monitoring services detect and report errors for operational monitoring and troubleshooting.

JSON [16] was chosen as a lightweight data-exchange format for communicating data records, and JSON schemas were defined to hold name/value pairs containing individual sensor measurements. For batch data extracts, both JSON and CSV formats are used to represent data in files that can be imported into spreadsheets and data analysis tools.

The same architecture and data-exchange platform was used to replicate the environmental sensing use-case to another city within the metropolitan region. This use case was chosen for its inherent heterogeneity in connectivity and power available at a given site. New sensors containing specially calibrated CO₂ sensors were quickly added to the environment using LoRaWAN connectivity. Real-time data from these sensors was then available to MQTT subscribing applications as well as through data extracts from the data-exchange platform. It is estimated that starting from scratch would have taken several weeks or more of detailed technical work; whereas replicating the existing architecture and implementation allowed the work to be completed within a day or two. Because the framework fundamentally focuses on reducing the barrier for secure information exchange (including earlier work by the team with the Data in Motion Exchange concept [17]), extending to new use cases or organizations requires significantly less effort. This is especially true if the data model is substantially similar to existing ontologies. Moreover, the use of the five messaging patterns in Figure 4 enable plugging into proprietary or preexisting Smart-City infrastructure through the bridging functions.

VI. Example Sensor Data

The primary purpose of our work is to create an IoT architecture that is replicable. However, to verify that the architecture is useful, several real-world installations were implemented as discussed in the Implementation section. For the first application, the architecture was implemented to allow the capture of sensor data from residential buildings to detect anomalies in daily living. These anomalies can be used to determine if a person needs medical assistance.

Figure 5 demonstrates a data stream from one of the environmental sensing installations. Sensor 8 is a multi-sensor device with LoRaWAN connectivity at an outdoor residential

location. This represents one of eight sensors that maintained longevity within the architecture. Table II shows the total sensed data over the first 9 months of collection. The number of elements is approximately 6 times more than the number of records; this is because each sensor collects multiple values.

VII. Discussion

The project successfully mitigated the barriers commonly found in the implementation of IoT solutions by cities and communities as introduced in section 3 (Methodology and Application.) The following subsections document the specific approaches that were adopted to address barriers encountered in this effort. A brief summary of each approach is provided in Table III.

Barrier 1 – Matching IoT Solutions to Use Cases

Given the newness of IoT solutions and the dearth of best practices, there is a need for better communication among government, industry and academia partners. The use of IoT in municipal governance often starts as a pilot proof-of-concept, some of which can be supported by multiple municipal partners. Involvement in pilot projects allows municipalities to 1) build experience with Smart-City and IoT architectures and technologies and 2) reduce the overhead of their own future implementations.

When the technology is not yet mature, a pilot program can inform them about future requests and contracts. If the technology is mature, but the return on investment is not yet clear, a pilot program can be used to make decisions with a higher level of confidence. In either case, these programs enable municipalities to better interface with the industrial partners who will perform the full implementation.

As part of our work, we studied several such pilot projects at various levels of maturity and investment. These pilots used a specific strategy involving low-cost, off-the-shelf technologies together with a highly flexible architecture, a common cloud, and a data backbone so that this infrastructure could be tailored to support pilots across a multitude of environments and use cases. Well-resourced local government leaders, impressed by vendor demonstrations, often leap to a different strategy: purchase expensive, large-scale, turnkey, hardware solutions that offer a tangible and fast road to implementation.

But this strategy often comes at a heavy cost. First, turnkey solutions are often designed for a narrow domain or purpose and implemented by individual government departments in a highly siloed manner. This makes it difficult for the municipality to develop a long-term, enterprise-level approach that ensures at least some level of interoperability, standardization, and, particularly, reuse and replication. Second, a jump to a single, vendor-led, turnkey solution limits the opportunities to learn about and develop a sufficient understanding of other, possible better, IoT solutions.

To avoid these risks and to increase our own capabilities, the project team, as noted above, very deliberately used its pilot funding 1) to learn first and implement at scale second and 2) to evolve a common data and cloud architecture. Our strategy was to rely on minimally

viable hardware solutions, which are based on open source and low-cost technologies. In this way, the team focused not on acquiring a grand solution up-front but rather on building out reusable components and a flexible architecture through rapid iterations.

There are several benefits of this approach. First, it provides a flexible, common infrastructure that can be tailored to suit a diverse range of use cases. Second, it allows users to explore and demonstrate which particular uses of the IoT-based solutions offered the most promise. Third, it exposes a broad range of community stakeholders to potential IoT opportunities. Fourth, this approach provides a foundational architecture, important lessons learned, an experienced in-house team, validated use cases, and buy in from key stakeholders. The result is a much more robust foundation for implementing sustainable, high-cost hardware at scale.

Barrier 2 – “Not Invented Here” Syndrome

The project encountered this barrier on several occasions. Each division of a municipality has 1) its own, internal, IT infrastructure and 2) a long-standing workforce that is often resistant to change. In our work, we utilized four strategies to combat NIH and resistance from internal departments.

1. Have the support of the organization’s leadership. Our work started with a smaller, targeted deployment under the auspices of a Chief Innovation Officer (CInO), who had a direct line to executive leadership at both the government-wide level and the individual department levels. The CInO acted as a central broker for multiple, IoT initiatives across diverse domains and departments.
2. Include input from domain experts within the organization. If stakeholders are being heard and included in discussions, then there is a higher likelihood of the department supporting and embracing the project. The CInO was crucial in building this buy-in through extensive discussions, outreach, and communication efforts. More importantly, these efforts were endorsed by the highest levels of the municipality’s government.
3. Use technologies that support both on-site and cloud-based deployments. The framework developed for this project is described abstractly, and can be implemented through structured components that can be hosted on a number of different platforms. Code containerization can allow collaboration on components across logical boundaries and provide a certain amount of scalability, but do require additional oversight to prevent inadvertent data breaches or incompatible new releases. Other technologies, such as OpenStack and CloudFoundry, offer Platform-as-a-Service or Infrastructure-as-a-Service technologies that allow users to create Virtual Machines, in on-premises servers, that are agnostic of the underlying system architecture.
4. Use a collection of smaller, service-based components. Large, monolithic applications with complete top-to-bottom architectures make reuse very difficult. Smaller components, alternatively, make it easier for individual services to be reused, replaced or adapted. Combining the service-component approach with a

common set of data-exchange patterns such as those in Figure 4 made it much faster to identify where existing components could be reused or replicated for new application use cases.

Barrier 3 – Communication and Collaboration across inter- and intra-organizational boundaries

The key to removing this barrier involves facilitating collaboration through information sharing and group learning. To this end, the project benefited from, and contributed to, two primary vehicles for collaboration: the NIST Global City Teams Challenge (GCTC) and the Thingststitute (discussed in more detail in the appendices). GCTC fosters peer learning and collaboration across jurisdictions. The Thingststitute is a government-run institution that facilitates local collaboration within both the local government and the local community.

A key lesson learned from this work is the *importance of successful messaging and branding*. This was inspired in part by peer efforts such as The Array-of-Things (AoT) project [18], [19], a collaboration between several institutions including Argonne National Laboratory, The University of Chicago, and the City of Chicago. AoT is investigating the use of urban computing and sensors and self-describes as a Fitbit for the city. The AoT sensors are a collection of smaller sensors, a wireless radio, and a processor with firmware that can be updated remotely.

Each sensor box does not necessarily contain the same set of sensing hardware. In fact, to have the same set of hardware in each sensor box would be costly while producing redundant data from parameters that do not change much over small geographic regions. However, explaining to all parties involved the contents of each sensor box and its installation location is burdensome, and can create a mixed message with the different configurations of hardware. In this instance, the benefits of crafting a common message and branding are clear.

Interested parties need only seek permission once, while providing budget and justification for the acquisition of those sensors. This allows for AoT boxes to be deployed with the right granularity for each sensor type, maximizing actual information while reducing total cost and roadblocks to the program. Following this strategy, the Thingststitute invested heavily in building brand equity for the Thingststitute and the SCALE (Smart Community Alerting Network) community sensing infrastructure. Our efforts in maintaining these collaborations are described in Appendix A.

Barrier 4 – Cybersecurity awareness and apprehension

To address the tendency for cybersecurity to be an afterthought, the team took a balanced approach to cybersecurity based on 1) understanding vulnerabilities and best practices, 2) assessing risks at each stage of development, and 3) steadily increasing the security robustness as components progressed from early stage exploration to later stage deployment.

This process was implemented in the design of the MQTT messaging infrastructure used to communicate SCALE data from sensor devices to back-end applications. During the preliminary stages of the design, work focused on sensor-device control, basic functionality,

connectivity, and use cases. MQTT was used to communicate data in an unencrypted, unauthenticated fashion. The results were functional and helpful in establishing a path forward. They did not, however, embody the robust security properties needed for broader deployment.

As the team moved SCALE forward to broader deployment, a more robust MQTT environment was needed. That environment was now required to detect traffic and behavioral anomalies. To meet those requirements, the eventual solution was based on encrypted MQTT communications, certificate-based mutual authentication, role-based security policies, and operational monitoring. Transitioning to this new MQTT environment allowed the team to start simple and then progressively add more security layers without having to change the underlying technology base.

Note, the solutions to none of these barriers is solely technical. Rather, these solutions will contain important business and organizational enablers that are similarly replicable and reusable across use cases and jurisdictions. Enablers that include business models, branding, communication and collaboration strategies, and peer learning approaches. Having such enablers included in the solutions will be valuable to overcoming the aforementioned barriers in complex institutions like municipalities.

VIII. Conclusion

The combination of IoT and smart cities has the potential to transform the way that people interact with their surroundings. However, the risk of entering into a new and unproved domain with a large investment can prove daunting for municipal leaders. This work expands on the effort of researchers and practitioners in the IoT and Smart City communities to reduce that risk by creating, testing, demonstrating, documenting, and disseminating technology that has been proven.

Specifically, this work built upon our own previous research to create a cybersecurity-aware standards-based set of components that can be used as a framework to build smart city solutions within organizations. The framework was informed by our existing work and discussions with other researchers, and is designed to 1) be technologically easy to replicate for new smart city implementations, and 2) abate common concerns (“barriers”) that cities have to implementation.

We note that the technology alone was not enough to reduce these barriers and additionally provide organizational insights for easing concerns. The framework was deployed to a live testbed, collecting multiple sources of data over several types of connectivity for three distinct projects over the course of eight months. In all, over 160 million distinct sensor records were produced by sensors and consumed by our system. To verify that the framework is replicable, an additional deployment within a different jurisdiction was created and is in operation.

Acknowledgement

Portions of this publication and research efforts are made possible through the support of NIST cooperative agreement #70NANB16H276.

Appendix A

Organization-based Collaboration

The NIST Global City Teams Challenge (GCTC) GCTC is a prominent example of recent efforts within the Smart-City community to bring municipalities together through expositions and collaborations both formal and informal. Perhaps equally important, the national recognition and spotlight provided by the GCTC and the credibility of its national partners makes it easier for local implementers, executive leadership, and the broader community to make a case for implementing IoT solutions.

This project made heavy use of these GCTC resources and assets. The initial work was in-part facilitated by researchers from the University of California, Irvine. Our later work included collaborations with the University of Maryland, Baltimore County, nearby municipalities such as Washington DC and Newport News, VA, and, several corporate entities. Bringing in these external parties helped us 1) facilitate conversations within the organization, 2) move past the NIH-type pushback from internal stakeholders, 3) identify best practices and promising use cases, 4) make use of industry partner experience and expertise, and 5) find reusable assets and partner-subsidized equipment.

At the local level, the Thingststitute provided similar functions. It convened key stakeholders for collaboration; promoted coordination, standardization, and joint learning; and, raised the visibility of IoT initiatives at the executive level and among the public. In providing these functions, the Thingststitute focused on 1) organizational and community engagement, facilitated by branding and 2) overcoming the confusion that often surrounds new innovations. Moreover, the existence of a dedicated, high visibility Thingststitute provided assurance to potential stakeholders of the governments commitment to serving as a sustained public sector IoT testbed.

The strategy for reducing technology confusion involved the implementation of pilots and deployments under the umbrella of a well understood, unifying brand for the governments IoT efforts. As part of the implementation team, we could focus on one of the critical roadblocks to any effective Smart-City (and, indeed, most IT) implementation: communication problems that result from the differing terminologies understanding, and interests of the different stakeholders in the project. Each municipality and organization will have its own politics and barriers to implementation. However, through our experience and that of peer organizations, it is strongly suggested to organize all Smart-City efforts underneath a single project name or formal designation with a recognizable brand or message. While there may be many similarities, the differences and uniqueness of a geographical region motivate the need for an extensible framework that is adaptable to needs. The basic communication patterns demonstrated in Figure 4 with an ontology based messaging model can be extended to suit most basic Smart City applications.

Biography

Alexander Nelson (M'13) received the BS degree in 2012 and the MS degree in 2013 in computer engineering from the University of Arkansas, Fayetteville, AR, and the PhD Degree from the Department of Computer Science and Electrical Engineering at the University of Maryland, Baltimore County (UMBC) under supervision of Nilanjan Banerjee and Ryan Robucci. He is an Assistant Professor of Computer Engineering at the University of Arkansas researching embedded real-time systems and pervasive computing. He is a member of the IEEE-HKN and Tau Beta Pi, and received the runner-up Best Demo Award at IEEE PerCom 2015 and an NSF GRFP Honorable Mention award. He is a member of the IEEE.

Greg Toth holds a BS in Electrical Engineering from the University of Notre Dame (1984) and a MS in Computer Engineering from the University of Southern California (1994). He has extensive experience in developing and deploying complex technologies in a variety of operational environments ranging from embedded systems to large-scale enterprises. He is the president of Tricarta Corporation and IoT Dev Labs, Inc., providing engineering design support to clients developing commercial electronic products, smart city applications, telecommunications infrastructure, and large-scale enterprise information systems. He is a member of the IEEE.

Dennis Linders holds a BA in Economics from the University of Florida (2003), a Masters of Public Policy from the University of Maryland (2008), and is a PhD Candidate at the University of Maryland's School of Information. Dennis is on the CountyStat team in the Office of the Montgomery County Executive where he helps local government executives use data to solve problems and improve government performance, particularly in the areas of customer service excellence, community analytics, inclusion, and environmental sustainability. He was previously with the World Bank's Urban Development global practice, where he helped cities learn from each other and contributed to data-driven national

urbanization strategies. His academic research focuses on data-smart cities, collaborative governance, and open government.

Cuong Nguyen joined the National Institute of Standards and Technology (NIST) in 2010 and leads the Smart Grid Testing and Certification Project in the Smart Grid and Cyber-Physical Systems Program Office of the Engineering Laboratory. He works with industry to support standards-based interoperability test programs to help accelerate smart grid deployments, and he also manages the NIST Smart Grid Advisory Committee. Cuong is the vice chair of the Smart Grid Interoperability Panel (SGIP) Smart Grid Testing and Certification Committee (SGTCC). In addition, Cuong coordinates international outreach efforts through bilateral and multilateral engagements.

Sokwoo Rhee is Associate Director of Cyber-Physical Systems Program at the National Institute of Standards and Technology (NIST). He is currently leading the Global City Teams Challenge (GCTC) which aims to create a replicable and scalable model for collaborative incubation and deployment of Internet of Things (IoT) and Cyber-Physical Systems (CPS) solutions to improve the quality of life in smart cities around the world. He previously served as a Presidential Innovation Fellow on CPS, a program by the White House Office of Science and Technology Policy. During his fellowship, he co-led the SmartAmerica Challenge, which brought together IoT technologies and CPS across the nation to demonstrate how they can provide concrete examples of the socio-economic benefits. Prior to joining US government, he was Co-founder and CTO of Millennial Net, Inc., which was one of the first to successfully commercialize low-power wireless mesh/sensor network and Internet of Things technology from academia. His work and achievements have been recognized through awards including MIT Technology Reviews Top Innovators under 35 and Red Herring's Top 5 Innovators. He holds more than a dozen US and International patents and numerous publications on wireless networks, biomedical sensors and embedded systems. He received his M.S. and Ph.D. in Mechanical Engineering from Massachusetts Institute of Technology.

References

- [1]. Burns MJ and Rhee S, "Facilitation of smart city and community technology convergence," in Proceedings of the 3rd International Workshop on Science of Smart City Operations and Platforms Engineering (SCOPE), 2018.

- [2]. "Smartamerica challenge: Harnessing the power of the internet of things," 2014, accessed June 14, 2018 [Online]. Available: <https://obamawhitehouse.archives.gov/blog/2014/06/10/smartamerica-challenge-harnessing-power-internet-things>
- [3]. "Smart america," 2014, accessed June 14, 2018 [Online]. Available: <http://smartamerica.org/>
- [4]. "Global city team challenge," 2018, accessed June 14, 2018 [Online]. Available: <https://pages.nist.gov/GCTC/>
- [5]. "Smart city framework – international technical working group on iot-enabled smart city framework," 2018, accessed June 14, 2018 [Online]. Available: <https://pages.nist.gov/GCTC/>
- [6]. Griffor ER, Greer C, Wollman DA, and Burns MJ, "Framework for cyber-physical systems: Volume 1, overview," Tech. Rep, 2017.
- [7]. Abdulkadir A, Mortamet B, Vemuri P, Jack CR Jr, Krueger G, Klöppel S, Initiative ADN et al., "Effects of hardware heterogeneity on the performance of svm alzheimer's disease classifier," Neuroimage, vol. 58, no. 3, pp. 785–792, 2011. [PubMed: 21708272]
- [8]. Ou Z, Zhuang H, Nurminen JK, Ylä-Jääski A, and Hui P, "Exploiting hardware heterogeneity within the same instance type of amazon ec2." in HotCloud, 2012.
- [9]. Denscombe M, The Good Research Guide: for small-scale social research. McGraw Hill, 2010.
- [10]. Kaplan RS, "Innovation action research: creating new management theory and practice," Journal of management accounting research, vol. 10, p. 89, 1998.
- [11]. Katz R and Allen TJ, "Investigating the not invented here (nih) syndrome: A look at the performance, tenure, and communication patterns of 50 r & d project groups," R&D Management, vol. 12, no. 1, pp. 7–20, 1982.
- [12]. Zuniga JC and Ponsard B, "Sigfox system description," LPWAN@IETF97, Nov. 14th, 2016.
- [13]. Alliance L, "Lorawan specification," LoRa Alliance, 2015.
- [14]. Hunkeler U, Truong HL, and Stanford-Clark A, "Mqtt-sa publish/subscribe protocol for wireless sensor networks," in Communication systems software and middleware and workshops, 2008. comware 2008. 3rd international conference on IEEE, 2008, pp. 791–798.
- [15]. "Node-red." [Online]. Available: <https://nodered.org/>
- [16]. Crockford D, "The application/json media type for javascript object notation (json)," 2006.
- [17]. Benson K, Fracchia C, Wang G, Zhu Q, Almomen S, Cohn J, Darcy L, Hoffman D, Makai M, Stamatakis J et al., "Scale: Safe community awareness and alerting leveraging the internet of things," IEEE Communications Magazine, vol. 53, no. 12, pp. 27–34, 2015.
- [18]. Beckman P, Sankaran R, Catlett C, Ferrier N, Jacob R, and Papka M, "Waggle: An open sensor platform for edge computing," in SENSORS, 2016 IEEE. IEEE, 2016, pp. 1–3.
- [19]. Catlett CE, Beckman PH, Sankaran R, and Galvin KK, "Array of things: a scientific research instrument in the public way: platform design and early lessons learned," in Proceedings of the 2nd International Workshop on Science of Smart City Operations and Platforms Engineering ACM, 2017, pp. 26–33.

Fig. 1.

A depiction of the iterative learning process based on Innovation Action Research used to drive the design and implementation of replicable smart city technologies.

Fig. 2.

A depiction of one of the IoT systems developed at the Thingstitute. This figure demonstrates a public-safety related system that detects the need for fire or ambulance at a senior living facility, and automatically routes a fire engine from the nearby volunteer department.

Fig. 3. A flowchart diagram demonstrating the architecture that was used to connect SCALE sensors to the cloud, and pass that data between logical units to perform real-time processing and alerting, as well as storage and historical analysis.

Fig. 4.

This figure demonstrates architectural patterns that are common, which represent the foundation of signal dissemination within our ecosystem. Sensors and actuators which can communicate over a publish/subscribe message broker schema such as MQTT follow the patterns in (a) and (b) for inbound and outbound traffic. Devices which are prebuilt with their own API (patterns (c) and (d)) should specify their data production and message consumption interfaces, which are controlled by applications either in the cloud or on-site. For environments that involve multiple cloud providers or vendor systems, bridging functions such as the two-way and three-way bridges shown in (e) are developed to tie the systems together.

Fig. 5.
Temperature, Humidity, and Pressure values (blue) and the daily average value (orange).

Fig. 6.

(Top) The Thingstutute logo used for denoting IoT efforts within the Montgomery County, MD Innovation Program. (Bottom) The SCALE logo, used to denote deployed IoT assets such as sensors and gateways.

TABLE I**Barriers to Replication Categorization**

Barrier	Barrier Category			
	Technological	Organizational	Political	Business
Match IoT Solutions to Use Case		X		X
Not Invented Here Syndrome		X	X	
Communication and Collaboration across organizational boundaries		X	X	
Cybersecurity awareness and apprehension	X	X	X	X

TABLE II

Environmental Sensor Statistics

Type	2017	2018	Total
Sensor Data Records	15,683,020	11,860,012	27,553,032
Sensor Data Elements	95,338,824	68,138,644	163,447,468

NIST Author Manuscript

NIST Author Manuscript

NIST Author Manuscript

TABLE III

Barriers to Replication – Approach Summary

Barrier	Approach Summary
Match IoT Solutions to Use Case	Pilot programs inform decision making. Model programs after successful peer organizations
Not Invented Here Syndrome	Achieve balance between downward pressure from leaders and inclusion of internal stakeholders.
Communication/Collaboration Across Boundaries	Utilize frameworks that allows cloud or on-site deployments and service-oriented components.
Cybersecurity Awareness and Apprehension	Organizational messaging and branding are vital. Maintain a single project moniker so smaller widgets are not viewed as standalone deployments with their own identity. Begin and end with security. All phases of the program require constant risk assessment and mitigation. Encrypt everything and do not rely on physical access security.