THE PRACTICAL SIDE OF IOT IMPLEMENTATION IN SMART CITIES

Artyom Kravchenko
St. John's University, USA

ABSTRACT

Smart cities are an innovative concept of sustainable urban design that gains popularity across the globe. Its core premise is the provision of smart educational, utility, traffic, waste and resource management, and health services with an advanced level of connectivity. The Internet of Things (IoT) is employed as the technology powering that connectivity and ensuring that the smart services operate based on intelligent data collection, sharing, and analysis. However, while IoT is actively explored today and exhibits numerous tech achievements, there are still pressing challenges for its practical implementation in the smart city architectures. This article explores the unresolved challenges such as impaired device interoperability, vulnerability of IoT grids to hacks, data security and privacy issues, as well as the slow transition of governments to smart services. The study also offers insights into the future directions of IoT research and development to empower smart city creation.

KEYWORDS

Internet of Things, Smart Cities, Smart City Grids, Interoperability, Smart City Architectures

1. INTRODUCTION

Smart cities are taking shape day by day to respond to the citizens' needs for enhanced liveability, safety, revivification, and sustainability. They represent hubs of smart services in the areas of education, government, mobility, housing, an e-health; these services are strongly interconnected mainly due to the application of Internet of Things (IoT) (Hassanien, Elhoseny, Ahmed, & Singh, 2018). IoT is an innovative technological concept presupposing a high level of connectivity and enhanced information sharing possibilities within the smart grid, as well as the increasing degree of smart devices' autonomy to take specific actions on their owners' behalf (Adekumbi, 2018). Due to these features, IoT is highly relevant to the principles of smart cities' design, and IoT tech is now actively integrated into the urban strategies. Smart city designers envision IoT-enabled applications as empowering the street and traffic lights, enabling smart transportation, parking, maintenance, waste management, air quality, crime reduction, architecture, sustainable energy usage and distribution, traffic flow, and addressing the pedestrian and bicycle needs (Meyers, 2017). However, IoT, as any other technology, poses certain issues and challenges in the process of practical implementation. This article explores the practicalities of IoT integration in smart cities and proposes solutions to streamline that integration more smoothly and effectively in the upcoming Smart City projects.

2. IOT-BASED SOLUTIONS FOR SMART CITY GRIDS

IoT has become a critical component of the smart city architecture right from its inception, which is explained by the fact that smart cities are first of all oriented at providing highly customized services to users. For instance, smart homes are enabled by effective data collection by electronic home appliances shared and stored in a smart home environment. Similarly, smart cities aim at advanced energy and electricity use, provision of a convenient and economically sustainable infrastructure for the social well-being, which becomes possible with IoT application (Hammi, Khatoun, Zeadally, Fayad, & Khouhi, 2017). At present, such sectors as energy and electricity, architecture and construction, automation, transportation, security, and healthcare are the key aspects unified by IoT in smart cities. All of them can be empowered by IoT to deliver service quality and

connectivity of a brand-new level, so the near future of smart city design deals specifically with the implementation of IoT in these spheres (Park et al., 2018).

In connection with such IoT objectives, the IoT platforms in smart cities have to be scalable due to the huge data storage requirements and, flexible to collect masses of miscellaneous data, and able to address the Big Data domain challenges. Thus, their key features include:

- Interoperability (enabling of communication and data transmission among heterogeneous IoT devices);
- Real-time data collection from a large number of sensors (fostering the provision of actual information about events or behaviors in the smart city);
- Near-real-time data transmission (implying the asynchronous communication enabled by the publish/subscribe communication paradigm);
- A microservice approach (presupposing the development of a single application as a suite of small services each running its own process and communicating with lightweight mechanisms);
- Awareness to end-users (IoT facilitates the interaction between users and things);
- Exposure of web services and API via open and standard data formats (fostering the design and development of novel services) (Patti & Acquaviva, 2016).

While IoT has already become a buzzword in the area of innovative urban design, there is still little understanding of the exact types of communication technologies expected to enable it. To date, the most suitable tech solutions for IoT in SCs include the power line communication (PLC) technology, ZigBee, WiMAX, third- to fifth-generation (3G-5G) cellular networks, the global system for mobile communication (GSM), general packet radio service (GPRS), and some more (Ejaz & Anpalagan, 2018). Since IoT is a modular approach, it is based on sensor integration (RFID, IR, GPS, laser scanners) into everyday objects to connect them over the Internet through specific protocols for information exchange, communication, and intelligent recognition, tracking, monitoring, and management (Saha, Auddy, Chatterjee, Pal, et al., 2017).

It is also noteworthy that for many, IoT is limited to connectivity of devices via the web, but the true implementation of IoT in smart cities is much broader. It suggests building a service based around the connectivity proposed to plug in with cloud integration and Big Data. IoT includes standards for connectivity, software, and even the clouds where the data is stored and processed. However, the implementation of IoT requires different control points and a variety of controlled parameters (Information Resources Management Association, 2018). Thus, the IoT technical architectures for smart cities require seamless integration of sensors in a mutual communication environment to create horizontal multiservice infrastructures and host all the city's systems. Such a task is challenging in many ways, and despite the technological advances of the recent years, the IoT sector still faces some pressing challenges as to the practical side of enabling smart cities.

3. CHALLENGES ON THE WAY TO AN IOT-ENABLED CITY

Since IoT is essentially about data retrieval, sharing, and storage, its critical weakness is vulnerability to hacks. Most connections in smart cities are enabled with RFID, which are highly vulnerable to all kind of hacking activities such as malware (a variety of harmful, dangerous computer programs such as worms, trojans, and viruses), ransomware (attacks on users with the purpose of money bribing), adware (attacks conducted to open ground for entering malware), etc. IoT grids also possess zero-day vulnerabilities (first-time system errors), side channels, phishing and spoofing, as well as RFID-related risks such as passive data monitoring, user identity scanning, and jamming of the RFID frequencies (Hassanien et al., 2018). Therefore, it is imperative to develop hack-proof IoT ecosystems to speed up the realization of smart city projects and to boost their development at a larger scale.

Another challenge inherent in the IoT architecture for smart cities is interoperability. While open standards have been in place for the past couple of decades, users still utilize interoperable systems rarely, which complicates scaling and a smart city's ecosystem creation. Various communication standards complicate the process of various processes' automation, as well as hinder the optimization, management, and reduction of accommodated energy. Even in the e-health sector of smart city services, the need to track medical team and facilities as well as healthcare-IT convergence services are imperative for the effective smart city functioning, which is hard due to the impaired interoperability (Park et al., 2018).

Security issues also play a role in the IoT implementation in smart cities because IoT systems are assumed to consist of very large heterogeneous networks of both constrained and unconstrained devices continuously operating without any power source. Because of these peculiarities, IoT architectures resist the implementation of strong security and privacy mechanisms. Major security challenges associated with IoT in smart cities include:

- Heterogeneity of communication technologies, software, hardware, and capabilities of multiple devices integrated into a single IoT grid;
- the constrained nature of numerous IoT devices possessing limited resources;
- the need to come up with scalable solutions to enable smooth IoT functioning at large-scale deployments;
- the need for energy-effective optimization in the use of IoT-empowering hardware and software (Angelakis, Tragos, Poehls, Kapovits, & Bassi, 2016).

Given these technical limitations inherent in the elements of an IoT grid, their creators face the challenge of balancing the system's agility and making it secure and privacy-preserving. According to the 2015 report of Hewlett Packard Enterprise, 90% of devices included in the IoT systems collect personal information, 70% of them use unencrypted traffic, and 60% of them have weak credentials (Rawlinson, 2015). Thus, no matter how secure the core IoT aspects are, the inherent weaknesses of peripheral devices may undermine the fundamental principles of user privacy and data protection.

Finally, it is noteworthy that while a transition from traditional cities to smart cities may be accelerated with the fast pace of technological development and disruptive technology's introduction in the global market, the path towards smart governments is much slower. Most often, governmental institutions and the public sector are the slowest to adopt new technologies, so the transition creates an unavoidable bottleneck on the way to establishing new smart city projects (Alenezi & Manuel, 2017). The modern-day imperative for the governments is to become more user-driven, responsive, flexible, and technology-oriented. Only after completing that evolutionary process, local and national governments may integrate into smart cities and complement them with innovative, technologically advanced governance.

infrastructures and host all the city's systems. Such a task is challenging in many ways, and despite the technological advances of the recent years, the IoT sector still faces some pressing challenges as to the practical side of enabling smart cities.

4. FUTURE DIRECTIONS OF IOT DEVELOPMENT IN SMART CITIES

IoT is already part and parcel of most smart city projects, powering the smart city technologies and infrastructure. Nevertheless, IoT also offers numerous additional business opportunities and possesses an enormous growth potential which may contribute to more efficient smart city development. To achieve greater progress with IoT in smart cities, recommendations for the future focus of developers include:

- prioritizing sensor-oriented technologies for wireless networking;
- developing technologies for network services;
- creating innovative energy-related technologies to power the energy load management technology, smart building energy management, and smart home cloud server technology.

Besides these recommendations for the industrial sector of IoT, technology needs for intelligent optimization, scheduling, and control of devices included in the IoT grids are pressing. Thus, the future of IoT development in smart cities is impossible without innovative solutions for intelligent collection, categorization, and analysis of Big data. Finally, IoT service provision may become more effective if employed via compatible integrated applications to ensure customization and end-user convenience (Park et al., 2018). Besides facilitating the development of smart city projects, numerous market players can embrace a promising business opportunity and increase their revenue by providing innovative solutions that the IoT requires.

5. CONCLUSION

As one can see, IoT is a highly promising aspect of smart city design without which the concept of connectivity and advanced end-user customization is simply unattainable. Thus, IoT is actively developed today, with new technologies emerging every day, to empower smart cities and make them sustainable socially, economically, and environmentally. Rapid technological advancement definitely contributes to the realization of smart city goals and visions, but the practical side of IoT implementation is still challenging in many ways. For instance, the implementation of most smart city projects is impossible without addressing such challenges as intelligent collection and analysis of big data, low interoperability, vulnerability of IoT grids to a wide range of attacks, and the lower speed of the public sector's technological advancement. Security still remains a pressing concern among smart city designers, so making IoT architecture work as it should presupposes the identification of IoT elements and assets requiring protection and development of system requirements for risk mitigation. The use of powerful encryption mechanisms and digital safety education for end users are also recommended steps to minimize the risks of hacking, data fraud, and data privacy breaches across the IoT grids in smart cities. Once these pressing issues are addressed and all aspects of smart city development are harmonized, smart city projects are projected to become more attainable and realistic.

REFERENCES

- Adekunbi, A., 2018. Three ways IoT is shaping the smart cities of the future. *Entrepreneur*. Retrieved from <https://www.entrepreneur.com/article/324345>
- Alenezi, A., & Manuel, P., 2017. Challenges of IoT based smart city development in Kuwait. *Thesis for Master of Information Technology*. DOI: 10.13140/RG.2.2.14375.04002
- Angelakis, V., Tragos, E., Poehls, H. C., Kapovits, A., & Bassi, A., 2016. *Designing, developing, and facilitating smart cities: urban design to IoT solutions*. New York, NY: Springer.
- Ejaz, W., & Anpalagan, A., 2018. *Internet of things for smart cities: technologies, big data and security*. New York, NY: Springer.
- Hammi, B., Khatoun, R., Zeadally, S., Fayad, A., & Khoukhi, L., 2017. Internet of Things (IoT) technologies for smart cities. *IET Research Journals* (September 2017), 1-14.
- Hassanien, A. E., Elhoseny, M., Ahmed, S. H., & Singh, A. K., 2018. *Security in smart cities: models, applications, and challenges*. New York, NY: Springer.
- Park, E., del Pobal, A. P., & Kwon, S. J., 2018. The role of Internet of Things (IoT) in smart cities: technology roadmap-oriented approaches. *Sustainability*, 10, 1-13.
- Patti, E., & Acquaviva, A., 2016. IoT platform for smart cities: requirements and implementation case studies. *2nd IEEE International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI 2016)*, Bologna, Italy, 7-9 September 2016, 1-6.
- Rawlinson, K., 2015. HP study finds alarming vulnerabilities with Internet of Things (IoT) home security systems. *Hewlett Packard Enterprise*. Retrieved from <https://www8.hp.com/us/en/hp-news/press-release.html?id=1909050>
- Information Resources Management Association, 2018. *Smart cities and smart spaces: concepts, methodologies, tools, and applications*. Hershey, PA: IGI Global.
- Meyers, R., 2017. Smart cities using Internet of Things solutions. *IIoT World*. Retrieved from <https://iiot-world.com/smart-cities/smart-cities-using-internet-of-things-practical-applications/>
- Saha, H. N., Auddy, S., Chatterjee, A., Pal, S., Sarkar, S., et al., 2017. IoT solutions for smart cities. *2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*. DOI: 10.1109/IEMECON.2017.8079565