TRANSFORMING HO CHI MINH CITY INTO A SMART CITY: AN IOT PERSPECTIVE

Le Quoc Cuong[*]

[*] Department of information and communications of Ho Chi Minh City

***Abstract*—This article addresses two important IoT considerations for Ho Chi Minh City's Smart city initiative: The need for an IoT platform and End-to-end security requirements for the IoT network. To provide context, the article will also provide background on the smart city initiative.

***Keywords*—smart cities, IOT, Ho Chi Minh City.**

I. THE GLOBAL MOVEMENT OF SMART CITIES AND TECHNOLOGY TRENDS

For decades, urbanization has been a phenomenon on the rise. Half of the world's population now resides in cities. By 2025, every two out of three people will probably live in urban areas [1]. This megatrend will continue into our foreseeable future, creating considerable stress upon aging city infrastructure and threatening effective governance. Developing cities are already showing signs of struggling to provide adequate housing, clean air and water, transportation, healthcare and other vital services to their citizens. To add to this conundrum, globalization poses new challenges to cities' competitiveness and their ability to attract sufficient investment to warrant growth.

Under these pressures, the traditional operating model for cities has begun to fall apart. Traditionally, cities used to spend duplicated efforts in vertical functional service departments. Citizens and businesses have to interact with multiple touch points and multiple layers of administration in order to obtain services. Information and data are locked within the respective departments that generated them, making it impossible to implement any holistic solution at speed.

Contrasting the old model, the modern operating model has been to integrate vertical silos, minimize service touch points, allow data to be shared and information timely communicated among departments, all of which can be combined and analyzed to provide new insights into the needs of citizens and businesses. Cities can now anticipate and solve problems with holistic and co-created solutions, at the same time realizing cost savings from shared infrastructure and resources [2]. The very process behind this new operating model is what we call "building a smart city."

Key to smart cities is data-driven decision making. Metcalfe's Law of network effects states that the level (or complexity) of connectivity determines the depth of insights that can be gathered (a.k.a. the value of the network). With growing sources, more information being shared will contribute to the accuracy and relevancy of all decision making processes in order to improve our livability and workability (from meeting our daily travel needs to knowing what is best to put on our breakfast table), to help businesses with product and service creation, to foster better governance and to drive economic growth while upholding our environmental responsibilities.

Yet even more exciting is how the Fourth Industrial Revolution (FIR) and the wave of digital transformation across industries and businesses are contributing to the global smart city initiative. With the FIR, we are advancing new technologies at an explosive rate in fields such as IoT, machine learning, data analytics, M2M communication and automation, virtual realities. With digital transformation, we are looking at entirely new business models where data plays a key role in nearly every stage of the value chain, revolutionizing the way entities engage their customers, empower their employees, optimize their operations, and transform their products and services [3]. The technology and the paradigm shift is all in alignment with the aforementioned smart city movement, making it quite reasonable to expect an explosive growth in the number of smart city projects until 2025 and beyond. As globalization is fast on its doorstep, Ho Chi Minh City simply cannot remain a bystander in this disruptive technological revolution.

Corresponding author: Le Quoc Cuong,
email: cuonglequoc@gmail.com

Manuscript received: 6/2017, revised: 8/2017, accepted: 8/2017.

II. TRANSFORMING HO CHI MINH CITY INTO A SMART CITY

Official numbers put Ho Chi Minh City at over 9.1% of the country's population while accounting for 28.7% of the national GDP. Ho Chi Minh City is the nexus of socio-economic growth and cultural diversity in Vietnam and the leading region within the top 7 city-provinces (Ho Chi Minh City, Ha Noi, Hai Phong, Da Nang, Binh Duong, Dong Nai, Can Tho), which altogether account for 52.6% of the national GDP, 71.4% of the country's budget income and over 50% of its export in 2015 [4]. It is easy to deduce that any problem or change affecting these major powerhouses would likely have a cascading effect upon the country itself.

Urbanization and population growth – mostly through migration – however, have created convoluting issues that have continued to worsen over the last decades. In 2016, the city's 10th Congress of the Party Committee have initiated 07 break-through programs aiming to address such issues, namely traffic congestion, pollution, urban flooding, quality of human resources, administrative reform, urban renovation and development, and improving economic competitiveness and development.

On the other hand, a steady rise in per capita income (PCI) during the last few years means higher demands for livability and service quality from city residents. In 2013, Ho Chi Minh City PCI was 4,513 USD. In 2014 and 2015, this figure reached 4,800 and 5.538 USD respectively (marking a 73% increase from 2010) [5]. In addition, the S.M.A.C (social, mobility, analytics, cloud) boom has been revolutionizing the way citizens connect, interact, voice their concerns, and contribute to bettering the city (over media like Facebook). These are citizen needs that the city also ought to meet.

The answer to these problems and needs is two-pronged, in that (1) the city must increase its management efficiency through horizontal integration, and (2) the city must be able to plan holistically and effectively. Both of these require data and ICT application on an unprecedented scale. Yet despite much ICT application progress having been made in city governance, data are currently not being adequately shared while a good portion of IT infrastructure remains siloed and under-utilized.

The smart city initiative appears to fit right in line with what is being sought. It will augment the current ICT deployment and those intended in the 07 breakthrough programs, providing the city with the capability to predict, plan, and execute well with a high level of integration. The City has drafted its Master plan (Figure 1 – see Appendix) to transform into a smart city, which employs an agile approach. As compared to the traditional waterfall approach, which demands the compilation of a detailed plan complete with all specific business, financial and actionable elements prior to implementation, the agile approach allows the city to start early from a minimal investment and quickly deploy simple solutions with immediate impacts (quick wins) – upon which continuous improvements can be made. The Masterplan therefore should not be viewed as a comprehensive catalogue of all smart city solutions that can be introduced to Ho Chi Minh City, but rather a general framework that guarantees flexibility and compliance with known and open standards plus a portfolio of solutions available for selection. Each functional department still retains the freedom to explore the availability of solutions in their respective field, yet they will do so with the benefits from a common ICT infrastructure and shared resources.

It should be noted that this strategic approach is consistent with the SCC's recommended ideal approach to transforming cities. The city's vision, guiding principles and objectives – which are shared and supported by all of its stakeholders – will act as top-down boundaries in project prioritization, selection and implementation. Meanwhile, an agile approach will allow the city to capture citizen inputs at various milestones during the execution stage – as they will be able to monitor the city's progress and provide feedback on what needs to be done.

The Smart city Masterplan has also drafted an open, interoperability-based ICT framework serving as the common foundation for all smart solutions (Figure 2 – See Appendix). Shared infrastructure and an open (shared) data platform can serve as a springboard for integrating the vertical dimensions of city governance, increasing productivity and efficiency, optimizing the city's budget, increasing transparency, encouraging citizen participation and providing opportunities for businesses and startups to capitalize on the city's data.

III. KEY NOTES ON IOT DELIVERANCE FOR THE CITY

As there are multiple technological topics that can be addressed from the various aspects of the abovementioned framework, we will focus instead on two key IoT considerations for the smart city plan: (1) The need for an IoT platform, and (2) End-to-end security requirements for the IoT network.

A. The need for an IoT platform

There are similarities among IoT reference architectures from several industry leaders [6][7]. Generally, an IoT architecture consists of things (devices, sensors), network (gateways and communication channels), and the back-end cloud (or platform) that provides data processing, deep analytics and management as well as business connectivity. The different standards being laid out for IoT can be pictured under a layered approach (Figure 3a – see Appendix) or under general architectural components (Figure 3b – see Appendix). It should be more visually convenient to go with a component-based architecture.

Several preliminary concepts need to be addressed. In this IoT setting, IP-capable devices can connect directly to a cloud gateway (not to be confused with a field gateway) in order to access the back-end cloud. Devices that use industry specific protocols (CoAP, OPC), short range communication technologies (Zigbee, Bluetooth), those simply unable to host a TLS/SSL stack or are not exposed to the Internet must go through a field gateway, which acts as a communication enabler that manages access and information flow (i.e. it can pass, or aggregate/streamline data before pushing some onto the cloud). Popular transport protocols and standards that should be supported include TCP (IETF RFC793), SCTP (IETF RFC4960), UDP (IETF RFC768), and UDT. Likewise, several popular messaging protocols that should be supported are the HTTP family (IETF RFC2818, HTTP/2 etc.) for "sporadic" communication, AMQP (ISO/IEC 19464:2014, OASIS) for long-lived connection with large data transmission, WebSocket (IETF RFC6455), MQTT (ISO/IEC 20922, OASIS MQTT 3.1.1) for constrained devices, CoAP (IETF RFC7252), and OPC Unified Architecture. For simplicity, we will not mention custom cloud gateways (that are sometimes used for protocol adaptation between the devices/field gateways and the cloud gateway).

The back-end cloud provides data processing, analytics, and management capabilities. Through provisioning APIs, it can govern devices' registration, removal, activation/deactivation, update and attestation through identity and registry stores, and metadata as well as operational data. The stream processor handles all data flow through the system in a broker mode (i.e. it decouples the sender and the receiver in such as a way to support multiple data consumers), to and from other components (storage, analytics, identity/state stores, app back-end and also business integration). The app back-end provides the business logic for the solution, frequently with stateless models or intrinsic-state models such as the actor framework such as Azure Service Fabric Reliable Actors, Java Virtual Machine-based Akka, and Akka.NET.

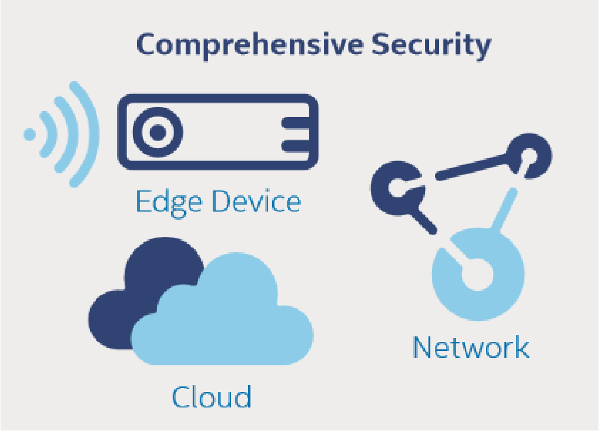

Figure 1 - Comprehensive security for IoT networks

As we can see, the complexity of standards and protocols being adopted across global industries creates a challenge for Ho Chi Minh City to address if it wants to follow a multi-vendor, interoperable approach. Meanwhile, the IoT solution roadmap is still being fleshed out as the plan moves forward. Therefore, it should be recommended that the city acquire an IoT platform (back-end cloud) from a top-tier provider that is open to international standard and protocol support, and on a subscription/pay-per-use basis. As for the IoT access network, it should not be centrally managed, but co-designed with solution providers as projects arise.

B. IoT end-to-end security

Also a top-priority issue for the IoT network is security – and it should be comprehensive security (Figure 4) across all aspects of the network, including edge devices, the communication network and the cloud. Protection should occur at all layers of the architecture (Figure 3a). At the cloud level, security is currently the most stringent. One of the most important provisions that the back-end cloud should consider is to employ best practices in device management, such as the separation of device registry and identity stores. At the network level, several things can be considered, one of which being the use of VPNs or a secure channel to add an extra layer of security to the communication between the edge network (including field gateways). Another mechanism that can be utilized is to enforce outbound-only communication for edge devices, which can be combined with an out-of-bound communication channel (such as mobile carrier SMS) to alert the device (which can then initiate an outbound connection to its home gateway). Device communication must be mutually authenticated at the transport and application layers, not the link layer.

And while most of the efforts have been spent to enhance security on data centers, clouds and networks, it was not until recently that IoT device security was identified as a primary cause for concerns. It has been widely known that cryptographic capability and attack resilience on IoT devices have been traded off for costs. This means that as the number of IoT devices grow exponentially, they will become easy targets for attacks due to a lack of security policy enforcement on both the software and hardware level. Hence several things must be required to better safeguard device interaction in untrusted spaces, for example:

- Devices will generally only establish outbound only communication to trusted or peered gateways. In the case that a device needs to receive commands from different services, the gateway must take care of information routing to verify that the commands come from authorized sources.
- Legacy devices with unsecure or nonstandard communication must connect to the cloud through a custom cloud gateway.
- The data encryption scheme should be provably secure, and broadly implemented (e.g. symmetric-key encryption like 128-bit AES). Similarly for digital signature, 128-bit SHA-2 should be considered.
- Support for TSL 1.2 (IETF RFC5246) for TCP communications, and optional support for TSL with PSK, X.509...
- Over-the-air updatable key-store and per-device keys with similar updatability for device firmware and application software.
- Physical tamper proofing: Cryptography-enabled microcontrollers, microprocessors or auxiliary hardware

such as TPM (Trusted Platform Module); secure boot loader and secured software loading in TPM; intrusion-detection via sensors, digitally self-destruction mechanism against physical manipulation etc.

It is the author's recommendation that the above suggestions should be taken into consideration when constructing the details guidelines for general IoT deployments within the city.

IV. CONCLUSION

The Fourth Industrial Revolution is hastening the digital transformation of cities worldwide into smarter cities, as disruptive technologies present both opportunities and challenges for governments and cities to adapt quickly to address their urbanization problems. With its aspiration to become a regional engine of growth, Ho Chi Minh City is embracing this opportunity with the creation of a Smart City Masterplan that serves as a general guidance for its coming journey, in the realization of which IoT plays a central role. As stated, this article has proposed several recommendations for the city regarding the development of an IoT platform and the importance of maintaining end-to-end security for the IoT system. The ability to effectively regulate and safely manage future IoT systems across the city will insulate the city from unnecessary expenditure and cyber threats.References

REFERENCES

[1] "World Urbanization Prospects - The 2014 Revision Highlights" (2014). United Nations, Department of Economic and Social Affairs (DESA), Population Division, pg 1.

[2] "PAS 181:2014 - Smart city framework – Guide to establishing strategies for smart cities and communities" (2014), British Standards Institution, pg 14.

[3] Digital Transformation. Microsoft Enterprise. <https://enterprise.microsoft.com/en-us/digital-transformation/>. Last accessed: April 18, 2017.

[4] Figures from the General Statistics Office and City annual reports.

[5] Figures from the General Statistics Office and City annual reports.

[6] The Intel IoT Platform – Architecture Specification White Paper.

[7] Microsoft Azure IoT Reference Architecture, 2016.

Le Quoc Cuong received his PhD. Degree from Peterburg university, Russia. Currently, he is a deputy director of the department of information and communications of Ho Chi Minh city. His reseach interests include optical networks and wireless communications focusing on IoT and cognitive radio.

Appendix – Figures

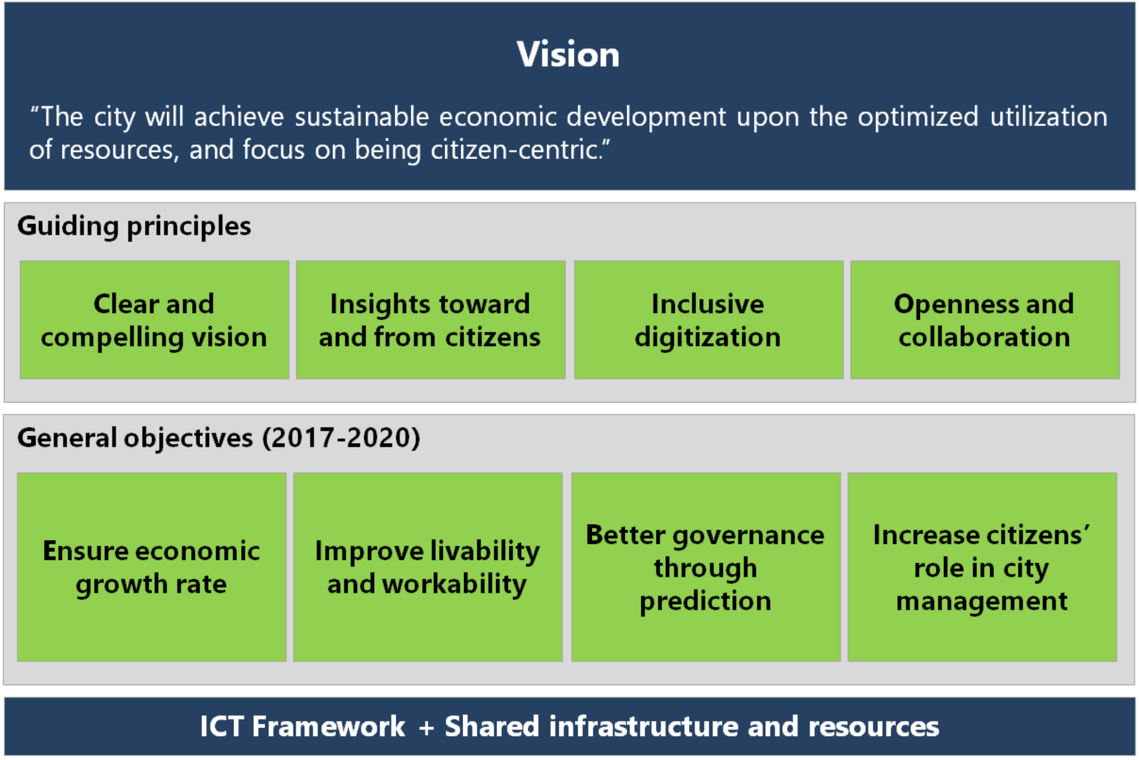
Vision
"The city will achieve sustainable economic development upon the optimized utilization of resources, and focus on being citizen-centric."
Guiding principles
Clear and compelling vision
Insights toward and from citizens
Inclusive digitization
Openness and collaboration
General objectives (2017-2020)
Ensure economic growth rate
Improve livability and workability
Better governance through prediction
Increase citizens' role in city management
ICT Framework + Shared infrastructure and resources

Figure 1 - Defining elements of the Smart City Masterplan

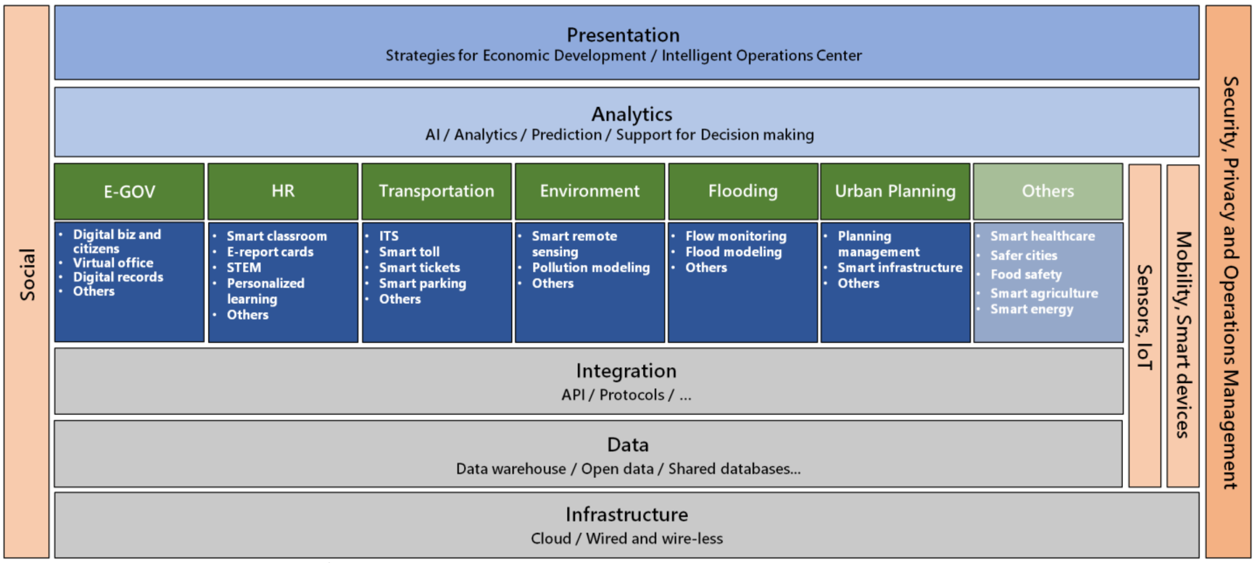

Figure 2. Smart City ICT Framework for Ho Chi Minh City

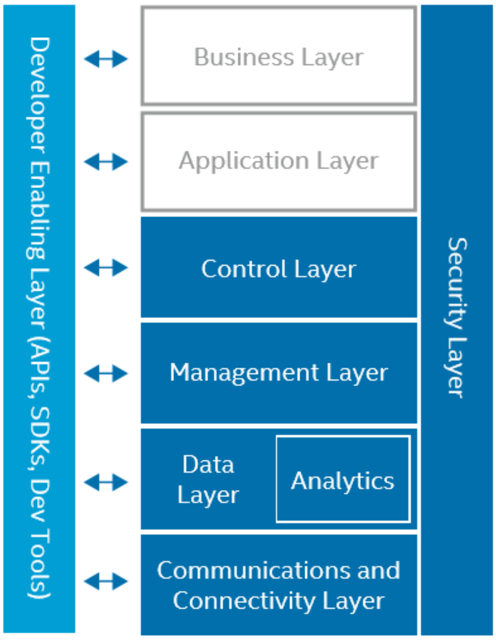

Figure 3a – Layered approach to IoT architecture

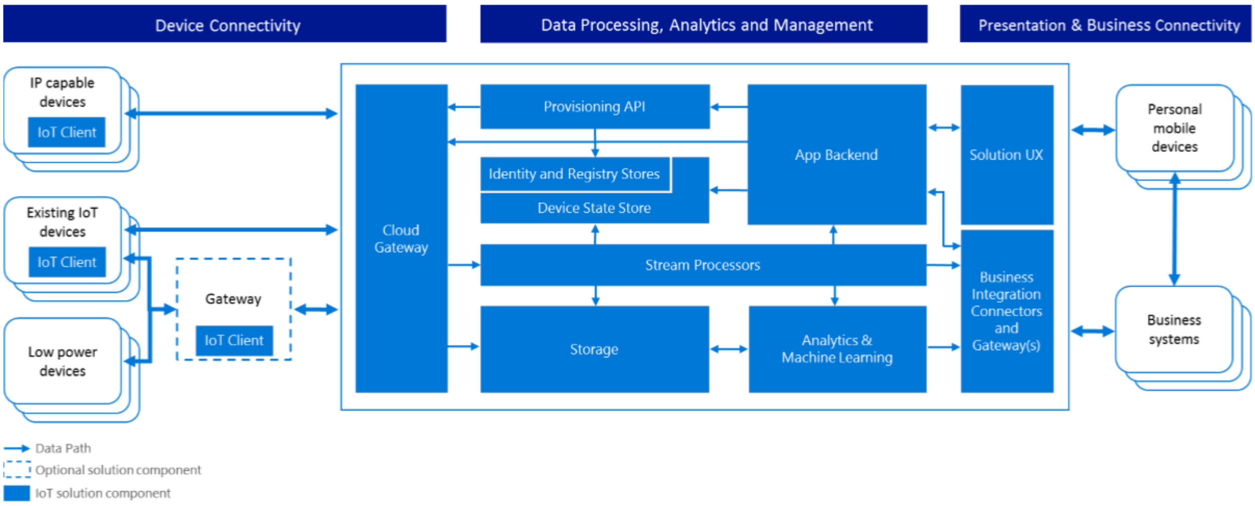

Figure 3b – Component-based approach to IoT architecture