A Reference Architecture for Smart and Software-defined Buildings

Manuel Mazzara[1], Ilya Afanasyev[1], Smruti R. Sarangi[2], Salvatore Distefano[3], Vivek Kumar[4], Muhammad Ahmad[3,5]
[1]Institute of Software Development and Engineering, Innopolis University, Russia
[2]Department of Computer Science and Engineering, IIT Delhi, India
[3]Dipartimento di Matematica e Informatica - MIFT, University of Messina, Messina, Italy
[4]NUST-MiSiS, Russia
[5]Department of Computer Engineering, Khwaja Fareed University of Engineering and Information Technology, Pakistan
{m.mazzara, i.afanasyev}@innopolis.ru, srsarangi@cse.iitd.ac.in, sdistefano@unime.it, {vivekkumar0416, mahmad00}@gmail.com

***Abstract*—The vision encompassing Smart and Software-defined Buildings (SSDB) is becoming more popular and its implementation is now more accessible due to the widespread adoption of the Internet of Things (IoT) infrastructure. Some of the most important applications sustaining this vision are energy management, environmental comfort, safety and surveillance. This paper surveys IoT and SSB technologies and their cooperation towards the realization of smart spaces. We propose a four-layer reference architecture and we organize related concepts around it. This conceptual frame is useful to identify the current literature on the topic and to connect the dots into a coherent vision of the future of residential and commercial buildings.**

***Index Terms*—Smart Cities, IoT, Building Operating Systems, Software Defined Systems**

I. Introduction

Smart and Software-defined Buildings (SSDB) represent the introduction of hardware, software, and sensing into the places where we live, in the same way as electronics has been introduced into cars and vehicles over the last twenty years. It is therefore the new frontier for what concerns housing solutions [1]. Advanced technology was introduced in cars in 80s initially in expensive models for then becoming the normality for small-size cars, and eventually legal frameworks adjusted in order to make formally mandatory the presence of certain sensing and acting functions [2]. In the same way, technology will possibly enter the market starting from high-end housing and public places to then move to more popular solutions. This paper surveys IoT and SSDB technologies and their cooperation towards the realization of Smart Cities and Smart Environments. We propose a four-layer reference architecture for SSDB and we organize related concepts around it. This conceptual frame is useful to identify the current literature on the topic and to connect the dots into a coherent vision of the future of residential and commercial buildings.

The manuscript is organized as follows: after this introduction, we first define Smart and Software defined Buildings (Section II), then discuss the hardware infrastructure (Section III) and the communication networks and protocols (Section IV) that are necessary for their realization. We then overview the SSDB management in Section V, their applications and services in Section VI and crosscutting concerns in Section VII. Finally, in Section VIII we present our conclusions.

II. Smart and Software Defined Buildings

Smart buildings (SB) are structures that use automated processes to control operations such as heating, ventilation, air conditioning, lighting, security, and allowing sophisticated monitoring and control over their functions [3]. One of the major set of functionalities that can be managed is the one concerning the *environment and users' comfort*. This includes temperature, light, and humidity. More complex functions can also be performed such as *presence monitoring, activity and identity recognition [4], and detection of users' emotional states* [5]–[8], under concomitant legal and ethical considerations. SB also represent an important element in a Smart City ecosystem, and are therefore often considered as drivers for the *urban smartization* process.

A Software Defined Building (SDB) [9] is a *"programmable"* building abstracting and virtualizing [10] the underlying (ICT) physical infrastructure to make it available (through specific API) for third party applications and services. SDB provide a *Building Service Layer* to implement an interoperable and programmable environment for their management and to control applications and services, following a software defined approach also adopted in Smart Cities [11]. Smart and Software Defined Building (SSDB) are two related concepts, even if not strictly dependent on each other. An SB can be either based on an SDB or not, and an SDB does not necessarily imply an SB. In the former case of an SB established on top of an SDB, specific SB services and applications for the building management are deployed on the SDB infrastructure by injecting their codes on the SDB programmable devices and nodes. An SDB-powered SB inherits the benefits of programmability from SDB, allowing to reuse and share existing physical resources and infrastructure through different services and applications. This allows that existing applications and services can be easily evolved and/or maintained or even extended with new ones, always exploiting the same SDB infrastructure.

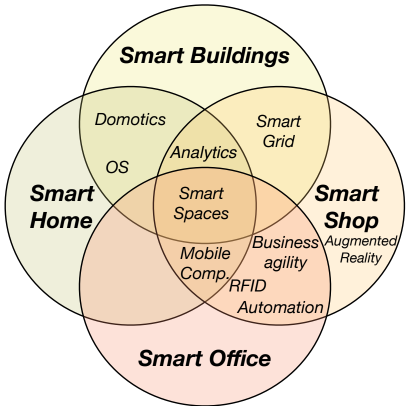

Fig. 1. Relationships among Smart Home, Office, Shop, Building concepts.

In the SSDB domain we can identify at least three different concepts that can be related to SB: *smart home*, *smart office* and *smart shop*. Their interactions and overlapping are shown in Fig. 1. The overall idea lying behind all these concepts is the one of *smart space*, i.e. a technology-equipped environment (residential, commercial, or governmental) that facilities life and operations of the people who are living it. *Domotics* and *Automation* are essential parts of smart spaces, as well as data management and *Analytics*.

SSDB Reference architecture

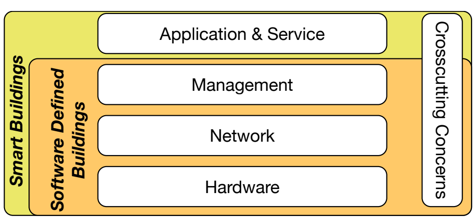

Fig. 2. Smart Building ICT Reference architecture

One of the contributions of this paper is the identification of a conceptual frame useful to organize concepts around the idea of SSDB. We propose a four-layer reference architecture shown in Fig. 2. At the bottom of the stack, the *Hardware* layer deals with all aspects related to the SSDB ICT infrastructure, ranging from devices, sensors, actuators, and IoT smart objects to network, storage, and processing hardware facilities deployed in the building for automation and smart management purposes. Such SSDB nodes, devices, objects, and things have to be properly interconnected, exploiting mechanisms and solutions provided by the *Network* layer. On top of the latter, the *Management* layer implements facilities for managing Smart Buildings ICT resources and data, dealing with interoperability issues arising from heterogeneous devices, as well as data management issues. Such mechanisms, technologies, and solutions allow to implement proper applications and services for a smart building such as those related to smart energy, surveillance, billing, and so on, which are grouped in the *Application & Service* layer. Finally, *Crosscutting Concerns* and issues such as security, privacy, AAA (authentication, authorization, and accounting), quality of service and similar, spanning the full stack of this Smart Buildings ICT architecture, are grouped altogether in the corresponding vertical layer. All such layers and modules are detailed in following sections.

The reference architecture of Fig. 2 covers both SDB and SB, highlighting their relationship. An SDB can mainly provide to an SB the ICT infrastructure, thus including the 3 bottom layers and the corresponding crosscutting concerns, while an SB also implements applications and services thus including the corresponding layer. As stated above, SB can even be deployed on SDB, by mainly injecting specific application codes on the programmable building infrastructure. Anyway, the SDB management level is usually more complex than the one of non SDB-powered SB, since it includes specific mechanisms for hardware abstraction through softwarization (API), and control mechanisms on top of this to manage, deploy and orchestrate tasks into pooled resources. This is often implemented through specific Building Operating Systems. In the remaining of the paper we will describe in details each layer above introduced.

III. Hardware

The hardware components that allow the management of the SSDB environment and the data collection are usually referred as *Internet of Things (IoT)*. The advantages of the introduction of this technology seem to overcome the disadvantages, and its application becomes easier every year since the price of hardware components is decreasing fast and the power of microprocessors is growing [12]. IoT kept growing for several years now [13]. It has been defined in multiple ways [14], but IoT is now usually used to refer to *a set of objects that are connected to the internet and can possibly communicate with each other via different protocols.* These objects are *sensors, actuators* and, more generally, *embedded systems*. Latest statistics state that there are around 22 billion of IoT devices in the the world [15] and enable the creation of a vast range of scenarios where devices communicate and cooperate [16]. These different scenarios regard many fields of our life, for example home automation, health, transportation and logistics. With regard to smart buildings, IoT sensing and actuation components can be categorized as follows:

Occupancy Detectors: these are specialized circuits that are placed in light bulbs, doors, and parking lots. They have dedicated motion sensors for sensing if there are individuals in the vicinity. If they detect motion, then the room is activated, which means switching on light bulbs, opening doors, and marking the parking slot as busy.

Positioning and Tracking: these sensors are put on individuals (e.g. bracelets or tags on clothes) or are located at different parts of a room to track the person's position. They are typically used to track the movements of geriatric patients. We can have specialized *activity detectors* that detect if a patient is falling down, or has suddenly become immobile.

Ambient Control Building automation is typically used in controlling the environment such as the air conditioning systems, heaters, humidity controllers, and for measuring the pollution, and ambient noise. They can be used to optimize the air conditioning cooling/heating only those parts of buildings that are populated. Most buildings with centralized air conditioning waste a lot of power because they assume that the entire building is constantly filled.

Measurement of Usage: home automation systems are being extensively used as of today to measure the consumption of electricity, gas, and water. The power bill or the water bill based on analyses of usage patterns.

Security: starting from early burglar alarm systems security has been an important user of home automation technologies. Modern smart homes have an array of sensors at important entry points, and integrate this information with the motion detected from CCTV cameras.

This wide variety of sensors, actuators and devices, is complemented by networking, storage and processing infrastructure facilities such as local switches, routers, NATs, and firewalls for networking, NAS and/or storage servers for storage as well as servers for processing. Of course, storage and processing servers could even be virtual or remote, provided by Cloud services.

IV. Networking

From a technical point of view, communication between devices is an important aspect in building automation systems [17], which can operate at different levels of abstraction. At the same time, a fully distributed system can be implemented in the building, in which the smart nodes interact only with each other to accomplish the task together. Given that the energy for communication is expensive, such peer-to-peer interactions are not preferable. Instead, the standard model is that the IoT nodes send their data to a centralized controller that collates all the data, performs some analysis, and then communicates with other upstream gateways.

Network protocols for Smart Buildings solutions are divided into smart device networks and traditional networks for high-speed data transfer. It is reasonable that smart building's devices will use the protocols already established in wireless sensor networks (WSN) and machine-to-machine communications (M2M). Since extending the functions in a protocol increases the cost and reduces usability, developing a suitable protocol is not an easy task and usually represents a trade-off between cost and performance. The mesh network is often the most suitable choice of network topology for wireless communication due to the presence of house obstacles, such as walls, furniture, etc. [18]. Double mesh (for wired and wireless networks) is well suited for buildings that had previously installed a wired home automation system. There are many communication networks and protocols for exchanging data with multiple devices, components, and sensors. Such protocols are created by various associations, consortia or private organizations, when a protocol is applied only by specific manufacturer(s) who must first obtain a license to use it. Commonly used communication protocols in smart buildings via wireless or wired meshes are described below [19], [20]:

InfraRed Data Association (IrDA): simple protocol, usually offering one-way communication. It has a limited range and requires direct visibility of a pair of receiver-transmitter.

Ethernet: Fast and robust wired communication with a range of up to 100m, enabling high noise immunity and the ability to power supply via cable for low power nodes.

UWB: an indoor short-range high-speed wireless communication (up to 10 m) with the bandwidth of over 110 Mbps (up to 480 Mbps), which can satisfy most multimedia applications, such as audio and video delivery in home networks.

WiFi: Fast and reliable wireless IPv6 (Internet Protocol version 6) with a transmission distance of about 25-50m (indoor). Its main feature is the existing broad support: almost every new electronic device comes with WiFi technology installed. As a rule, this is a upper level protocol, where IP is the most predominant protocol that allows communications over the Internet without using a protocol translator.

WLAN: Wireless local area network (WLAN), also known as Wireless Ethernet, is capable to provide reliable communication with low latency for both point-to-point and point-to-multi-point transmissions up to 250m. WLAN applies spread spectrum technology, so users can occupy the same frequency bands with minimal interference to each other.

Bluetooth: a short-range wireless protocol (up to 10 m), the main features are low power consumption (especially Bluetooth low energy - BLE) and fast data exchange, as well as widespread availability. Its adaptive frequency hopping system detects existing signals, such as WiFi, and coordinates the channel map for Bluetooth devices to minimize interference. It also implements node discovery services.

6LoWPAN: the IPv6 low power adaptation for devices with limited resources, combining the advantages of both IP and Bluetooth and enabling mesh networks for energy-saving applications in smart buildings with a distance up to 200m.

Thread: the IPv6-based, low-power technology for IoT networks designed to provide security and meet future requirements. The specification of the Thread protocol is available free of charge, however, this requires consent and permanent adherence to the license agreement. Thread exploits 6LoWPAN, which is based on the use of a connecting router, called an edge router. This means that 6LoWPAN does not know about application protocols and changes that reduces the load on the computing power at the edge routers. Thread is designed to exchange data between devices, even when the WiFi network is turned off.

Zigbee: a wireless mesh network that has proven its efficiency and thrift when expanding the network, having a transmission distance of 10-75m. ZigBee offers low data rates for personal area networks (PAN). It can be widely used in device control, reliable messaging, building automation, consumer electronics, remote monitoring, healthcare, etc.

Z-Wave: a mesh network protocol standard designed for remote control applications in residential and business areas, whose bandwidth is about 6 times lower than for Zigbee.

This, however, requires less energy to cover the same range as Zigbee. The advantages of the technology come from a simple command structure, the absence of internal interference, low-frequency bandwidth control, and IP support. Z-Wave usually has a range of 30m indoors, which extends to 100m outdoors.

KNX: one of the most popular open protocols for automation. It operates on several physical levels, such as twisted pair, network power line, infrared, Ethernet and RF channel. Subscribers (devices) connected to the bus (network) can exchange data over a common transmission channel (bus). Then the data is packed in a telegram and transmitted via a cable from a sensor to actuators. After successful transmission and reception, each receiver confirms the telegram delivery, otherwise the transmission is repeated only two times. If there is no confirmation, the transfer process ends. That is why the KNX protocol is not used in the critical applications. In a decentralized topology, KNX does not work from a central unit and each unit is connected to the smartest device of the KNX ecosystem without dependence on the functioning of other parts. Thus, if one unit fails, others continue to work.

V. Management

The Smart Building Management layer is in charge of managing the ICT infrastructure. Management functionalities form two groups: resource management and data management.

A. Resource Management

Smart buildings are "melting pots" of heterogeneous technologies, especially for sensing and actuation devices. To deal with such heterogeneity issues in Smart buildings, specific solutions have been developed, mostly in form of operating systems. In this direction *building management system* (BMS) or *building automation system* (BAS) [21] were implemented providing an automation solution for controlling heating, ventilation and air conditioning (HVAC), security, fire alarm, power, water supply and elevator systems in a coordinated way. Extending the scope beyond automation, some attempts in defining more general *building operating systems* (BOS) have been performed, most of them reported and compared in [22], which also proposes a quite advanced BOS solution named XBOS. However, among them, one of the most relevant is the Building Operating System Services (BOSS) [23], since it defined a new approach to deal with smart buildings: through programmable buildings. This way, the idea of SDB is slowly affirming in the smart building context, even if its potential is still untapped and not fully investigated. Even the concept of virtualization and virtualized buildings have been recently defined in [10], but there is still room for *Building Function Virtualization (BFV)* and new *Virtual Building Functions (VBF)*. The basic design philosophy of a building's operating system is the plurality of possibly unrelated applications, high requirements of fault tolerance, and a very flexible specification for interacting with many applications. Some of the major issues that need to be addressed with BOS are interoperability, planning, placement, pooling, and orchestration.

B. Data Management

The storage and analysis of Smart Building data is challenging in several ways. First, due to the diversity of technologies and systems [24], the building automation technique faces a long relation with interoperability, leading to data integration concerns [25]. Secondly, for a better perception and control of instruments, the density of sensors, promptly increases, generating a vast amount of data. Bashir et al. [26] propose a big data analytic framework for smart buildings. Let's divide a typically data processing architecture into several layers.

Sensor layer: This layer consists of sensors that generate data, and record ambient parameters.

Data storage: This information is communicated to routing nodes that collect the data and store it. In [26] TCP-based protocol for communicating data and storing it in a cloud based database was proposed. Often no-SQL databases are used to store such streaming data such as Apache Flume, and HDFS.

Analytics: Some of the common engines that are used on such platforms are based on the classic Spark toolkit such as PySpark. PySpark can be used to set alerts and thresholds, e.g. once the level of oxygen dips in a room, oxygen pumps can automatically start operating.

Rule Engine: This is an engine that has a set of pre-written rules. Every rule has a set of pre-conditions, and a set of actions. If the conditions for firing a rule exist, then the rule is fired, and appropriate action is taken.

Visualization: The last component, where users can visualize all the elements in the SSDB, the data that are generated, and the actions that are being performed.

VI. Applications, Services and Ambient Intelligence

From an end-user/application perspective, the idea of SB belongs to a wider concept: Ambient Intelligence (AmI) [27]. According to AmI vision, the environment is able to anticipate the needs of its inhabitants therefore responding in a timely and user-friendly way. Implementing the vision of AmI is highly ambitious, but to reach this goal it is necessary to realize at least a basic set of services that should be part of Smart Buildings' behavior. In this section, we will discuss the main application and services that Smart Building should offer towards this vision. We identify three major areas where benefits may soon appear: Energy Management, Environmental Comfort and Safety, and Surveillance.

A. Energy Management

Given rising energy costs, energy management in modern buildings is vitally important. Almost all new constructions need be *green* buildings. The reasons are that modern buildings consume a lot of energy, which can be reduced by efficient management. Consumption in residential buildings accounts for about 40% of the total energy consumption in the world. In comparison, commercial and business buildings (offices, shops, shopping malls, hotels, etc.) and spaces with public functions (schools, hospitals, etc.) use approximately 30% of energy resources [28]. In recent years, the growth in the number of energy standards and certifications has made the reduction of energy consumption more urgent. At the same time, rising energy costs have made efficient energy management a matter of survival. It is not surprising that in such a growing market the major IT corporations have realized the importance of building automation, in particular concerning the energy management. Intel, for example, provides an IoT platform with analytics to offer building operators and managers the possibility of keeping systems functional and cost-effective [29]. The Nokia smart building energy management application has been designed to monitor and control critical building systems and ensure efficient operation. Reports and alerts help managers identify areas where the observed high energy consumption can be optimized [30]. Academic research has also focused on identifying open issues and possible solutions [31], [32] and characterizing energy management systems (EMS) [33]. An energy management system is defined as *a computer-aided tool used by operators of electric utility grids to monitor, control, and optimize the performance of the generation and/or transmission system*. Some researchers have proposed approaches and technologies for the operation of energy management systems for smart homes [34].

A *Home/Building Energy Management System (H/BEMS) is a system that incorporates sensors in household appliances through a home/building network to optimize energy consumption*. Most of the academic and industrial solutions are defined according to a general architecture for H/BEMS. This is composed of a *Home/Building Area Network (H/BAN)*, a local residential network interconnecting devices (sensors, smart plugs, intelligent thermostats, cameras). It could be a wireless wired network. Then, *Monitoring and Control Devices* are responsible for monitoring and controlling the energy consumption of appliances and devices. *Processors* are in charge of concentration, storage and management of the information. The server and the database are in this central module. *Gateways* ensure connection between the H/BEMS and the outside to allow remote access.

B. Environmental Comfort

The basic function of Smart Building is to regulate environment parameters such temperature, humidity, lightning to maximize comfort. This problem has been considered in literature in non-trivial way. For example, in [35] a dynamic thermal model of occupants has been proposed. The model is based on the heat balance equation of human body and thermal characteristics of the occupants. In the context of Smart Offices, occupant satisfaction with indoor environmental conditions has been studied in [36]. This application area is broader than just regulating temperature and similar parameter. Although some results of environmental regulation should be immediate and quickly perceived, sometimes the well-being of residents can depend on a larger number of factors. In [37] the authors introduced a real system deployed in the offices of four Microsoft campuses in China to monitor indoor air quality enabling employees to enquire the air quality of a place by using a mobile phone or checking a website.

C. Safety and Surveillance

Maximal safety conditions are guaranteed by Smart Buildings through surveillance operated by IoT technology. Cameras are just one of the main surveillance tools, but certainly not the only one. Access authorization can be performed via biometric parameter and face recognition can be used for security reason. It is important to emphasize that, although the device infrastructure is an important element to ensure safety, it is the software playing a major role here. In [38] the authors realized that information provided by single sensor and surveillance technology may not be sufficient to understand the whole context of the monitored environment, and therefore propose the Smart Building Suite, where independent and different technologies are developed in order to realize a multimodal surveillance system.

VII. Crosscutting concerns

Crosscutting Concerns are issues spanning the full stack of our reference architecture. Each of these would require a separate investigation. Given the limited space we will here scratch the surface and identify two of these concerns:

Security: The more a building is connected the more security threats it is subject to. Given the experiences with automotive or other devices, building owner may be aware of it [39], [40]. The problem has to be addressed from two different point of view: technical and communication.

Adaptability: Information internally and externally gathered from a range of sources can be used to prepare buildings for a particular event before that event actually happens [41]. This is a radical shift from the idea of *reactive* building to the one of *proactive*. Smart Buildings should be adaptive. For example a building can adapt to different times of year and different people's perceptions of comfort.

VIII. Conclusions

In this paper we surveyed SSDB and related technologies, and looked into the major solutions proposed by industry and academia. We would like here to emphasize the major concerns for the widespread adoption of such technologies:

Skilled Operators: people do not know the existence of the described frameworks. In general, operators have no experience and skills in managing Smart Buildings and analyzing large amounts of performance data. Even adopting the technology, it will take a significant training effort before operating buildings in the optimal way [42].

Costs of startup and maintenance: installing such technologies and maintaining them is at the moment expensive and we are not aware of tax incentives in most of the countries. Without some kind of incentives it will be hard to convince building owners that the investment is worth the cost, especially for small- and medium-sized buildings [43].

Interoperability: as mentioned before in this paper, not all smart devices are interoperable with each other and making things work could be a challenge. Standard protocols to connect all devices do not exist at the moment [3].

There are some aspects that we did not cover here, although they deserve a separate discussion. First, "Autonomous Cars" and "Smart Buildings" are two emerging technologies that are destined to cooperate [44], [45]. Second, the use of micropayments and financial interactions between smart entities most likely via blockchain will soon become a stimulating highway for digital economy and smart cities [46]–[48].

References

[1] "Smart buildings: Forming the foundation of smart cities." www.forbes.com/sites/insights-inteliot/2018/10/24/smart-buildings-forming-the-foundation-of-smart-cities/. Accessed: 2018-02-09.

[2] "The role of electronics in automotive advancements." https://auto.howstuffworks.com/car-driving-safety/safety-regulatory-devices/new-technologies-cars-less-safe1.html. Accessed: 2018-02-09.

[3] A. Khusnutdinov, D. Usachev, M. Mazzara, A. Khan, and I. Panchenko, "Open source platform digital personal assistant," in *WAINA*, 2018.

[4] M. Ahmad, A. M. Khan, M. Mazzara, and S. Distefano, "Seeking optimum system settings for physical activity recognition on smartwatches," in *2019 Computer vision conference (CVC'19)*, 2019.

[5] M. Ahmad, A. Khan, J. Brown, S. Protasov, and A. Khattak, "Gait fingerprinting-based user identification on smartphones," in *IJCNN*, 2016.

[6] M. Ahmad, M. A. Alqarni, A. Khan, A. Khan, S. H. Chauhdary, M. Mazzara, T. Umer, and S. Distefano, "Smartwatch-based legitimate user identification for cloud-based secure services," *Mobile Information Systems*, vol. 2018, pp. 5107024:1–5107024:14, 2018.

[7] M. Ahmad, A. M. Khan, M. Mazzara, S. Distefano, A. Ali, and A. Tufail, "Extended sammon projection and wavelet kernel extreme learning machine for gait-based legitimate user identification on smartphones," in *ACM Symposium On Applied Computing (SAC19)*, p. 4, 2019.

[8] M. Nalin, I. Baroni, and M. Mazzara, "A holistic infrastructure to support elderlies' independent living," *Encyclopedia of E-Health and Telemedicine, IGI Global*, 2016.

[9] S. Dawson-Haggerty, J. Ortiz, J. Trager, D. Culler, and R. H. Katz, "Energy savings and the software-defined building," *IEEE Design Test of Computers*, vol. 29, pp. 56–57, Aug 2012.

[10] M. A. Abid and H. De Meer, "Virtualized software defined buildings: a key enabler of the future smart cities," in *SmartGridComm*, 2018.

[11] G. Merlino, D. Bruneo, F. Longo, A. Puliafito, and S. Distefano, "Software defined cities: A novel paradigm for smart cities through iot clouds," in *IEEE Workshops UIC-ATC-ScalCom*, pp. 909–916, 2015.

[12] D. Salikhov, K. Khanda, K. Gusmanov, M. Mazzara, and N. Mavridis, "Jolie good buildings: Internet of things for smart building infrastructure supporting concurrent apps utilizing distributed microservices," in *1st Int. Conf. "Convergent"*, pp. 48–53, 2016.

[13] "Iot platforms: Market report 2015-2021." https://iot-analytics.com/product/iot-platforms-market-report-2015-2021-3/. Accessed: 2018-02-09.

[14] J. Santos, J. J. P. C. Rodrigues, J. Casal, K. Saleem, and V. Denisov, "Intelligent personal assistants based on internet of things approaches," *IEEE Systems Journal*, vol. 12, pp. 1793–1802, June 2018.

[15] "Internet of things (iot) connected devices installed base worldwide from 2015 to 2025 (in billions)." https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. Accessed: 2018-02-09.

[16] P. Mekikis, A. Antonopoulos, E. Kartsakli, A. S. Lalos, L. Alonso, and C. Verikoukis, "Information exchange in randomly deployed dense wsns with wireless energy harvesting capabilities," *IEEE Transactions on Wireless Communications*, vol. 15, pp. 3008–3018, April 2016.

[17] D. Salikhov, K. Khanda, K. Gusmanov, M. Mazzara, and N. Mavridis, "Microservice-based iot for smart buildings," in *Int. Conf. WAINA*, 2017.

[18] B. Stojkoska and K. Trivodaliev, "A review of internet of things for smart home: Challenges and solutions," *J. Clean Prod.*, vol. 140, 2017.

[19] "Smart home protocols explained." https://medium.com/iotforall/smart-home-protocols-thread-zigbee-z-wave-knx-and-more-71efa4b410e1. Accessed: 2018-02-09.

[20] G. Lobaccaro, S. Carlucci, and E. Löfström, "A review of systems and technologies for smart homes and smart grids," *Energies*, vol. 9, no. 5, p. 348, 2016.

[21] P. Domingues, P. Carreira, R. Vieira, and W. Kastner, "Building automation systems: Concepts and technology review," *Computer Standards & Interfaces*, vol. 45, pp. 1–12, 2016.

[22] G. Fierro and D. E. Culler, "Xbos: An extensible building operating system," in *BuildSys*, pp. 119–120, ACM, 2015.

[23] S. Dawson-Haggerty, A. Krioukov, J. Taneja, S. Karandikar, G. Fierro, N. Kitaev, and D. Culler, "{BOSS}: Building operating system services," in *USENIX Net. Sys. Design & Impl. (NSDI 13)*, pp. 443–457, 2013.

[24] J. Ploennigs, "A modular, adaptive building automation system ontology," in *38th Ann. Conf. on IEEE Industrial Electronics Society*, 2012.

[25] M. Moreno, "Applicability of big data techniques to smart cities deployments," *IEEE Trans. on Industrial Inf.*, vol. 13, pp. 800–809, 2017.

[26] M. R. Bashir and A. Q. Gill, "Towards an iot big data analytics framework: smart buildings systems," in *Int. Conf. on HPCC/SmartCity/DSS*, pp. 1325–1332, IEEE, 2016.

[27] F. Sadri, "Ambient intelligence: A survey," *ACM Comput. Surv.*, vol. 43, no. 4, pp. 36:1–36:66, 2011.

[28] "How iot technology is changing building energy management systems." https://internet-of-things-innovation.com/insights/the-blog/how-iot-technology-is-changing-building-energy-management-systems/. Accessed: 2018-02-10.

[29] "Smart building energy management solutions." https://www.intel.com/content/www/us/en/energy/solutions/smart-building-energy-management.html. Accessed: 2018-02-09.

[30] "Nokia smart building energy management." https://internet-of-things-innovation.com/iot-solutions/smart-building-energy-management/. Accessed: 2018-02-09.

[31] P. Rocha, A. Siddiqui, and M. Stadler, "Improving energy efficiency via smart building energy management systems: A comparison with policy measures," *Energy and Buildings*, vol. 88, pp. 203 – 213, 2015.

[32] M. Fahim and A. Sillitti, "Analyzing load profiles of energy consumption to infer household characteristics using smart meters," *Energies*, vol. 12, no. 5, p. 773, 2019.

[33] I. D. Serna-Surez, G. Ordez-Plata, and G. Carrillo-Caicedo, "Microgrid's energy management systems: A survey," in *EEM*, pp. 1–6, 2015.

[34] M. Shakeri, M. Shayestegan, H. Abunima, S. S. Reza, M. Akhtaruzzaman, A. Alamoud, K. Sopian, and N. Amin, "An intelligent system architecture in home energy management systems (hems) for efficient demand response in smart grid," *Energy&Buildings*, vol. 138, 2017.

[35] H. Park and S.-B. Rhee, "Iot-based smart building environment service for occupants thermal comfort," *Journal of Sensors*, 2018.

[36] A. Aryal, F. Anselmo, and B. Becerik-Gerber, "Smart iot desk for personalizing indoor environmental conditions," in *8th Int. Conf. on IoT*, IOT '18, pp. 35:1–35:6, ACM, 2018.

[37] X. Chen, Y. Zheng, Y. Chen, Q. Jin, W. Sun, E. Chang, and W.-Y. Ma, "Indoor air quality monitoring system for smart buildings," in *Int. Conf. on Perv. & Ubiq. Comp.*, UbiComp, pp. 471–475, ACM, 2014.

[38] G. Amato, P. Barsocchi, F. Falchi, E. Ferro, C. Gennaro, G. R. Leone, D. Moroni, O. Salvetti, and C. Vairo, "Towards multimodal surveillance for smart building security," *Proceedings*, vol. 2, no. 2, 2018.

[39] N. Dragoni, A. Giaretta, and M. Mazzara, "The internet of hackable things," in *Adv. in Intel. Sys. & Comp.*, vol. 717, pp. 129–140, 2016.

[40] M. D. Donno, N. Dragoni, A. Giaretta, and M. Mazzara, "Antibiotic: Protecting iot devices against ddos attacks," in *SEDA*, vol. 717 of *Adv. in Intel. Sys. & Comp.*, pp. 59–72, Springer, 2016.

[41] A. Buckman, M. Mayfield, and S. BM Beck, "What is a smart building?," *Smart & Sustain. Built Envir.*, vol. 3, no. 2, pp. 92–109, 2014.

[42] "Smart operators for smart buildings." http://www.cunybpl.org/wp-content/uploads/2017/11/Smart-Operators-Smart-Buildings.pdf. Accessed: 2018-02-10.

[43] "How to conquer common smart building hurdles." https://www.buildings.com/article-details/articleid/21098/title/scale-the-smart-technology-barriers. Accessed: 2018-02-10.

[44] D. Strugar, R. Hussain, M. Mazzara, V. Rivera, I. Afanasyev, and J. Lee, "An architecture for distributed ledger-based m2m auditing for electric autonomous vehicles," in *33rd Int. Conf. WAINA*, 2019.

[45] R. Gmehlich, K. Grau, A. Iliasov, M. Jackson, F. Loesch, and M. Mazzara, "Towards a formalism-based toolkit for automotive applications," in *Formal Methods in Software Engineering (FormaliSE)*, 2013.

[46] C. Lazaroiu and M. Roscia, "Smart district through iot and blockchain," in *ICRERA*, pp. 454–461, Nov 2017.

[47] S. Lonshakov, A. Krupenkin, A. Kapitonov, E. Radchenko, A. Khassanov, and A. Starostin, "Robonomics: platform for integration of cyber physical systmes into human economy," 2018.

[48] I. Afanasyev, A. Kolotov, R. Rezin, K. Danilov, A. Kashevnik, and V. Jotsov, "Blockchain solutions for multi-agent robotic systems: Related work and open questions," *arXiv preprint arXiv:1903.11041*, 2019.