Evaluation of IoT Device Management Tools

Biliyaminu Umar[1], Hamdan Hejazi[1], László Lengyel[1], Károly Farkas[1,2]
[1]Budapest University of Technology and Economics,
[2]NETvisor Ltd
email: biliyaminu.umar@edu.bme.hu, hamdan.hejazi1@gmail.com, lengyel@aut.bme.hu, farkask@hit.bme.hu

***Abstract*— Industry 4.0 with Internet of Things (IoT) is the next wave in technology revolution, which is expected to change our everyday life. This digitalization is having great impact on all the domains (energy, healthcare, transportation, manufacturing etc.) in addition to the Information and Communication Technologies (ICT) sector. In IoT scenarios, numerous sensors measure and report several phenomena and diversified IoT solutions are deployed to collect huge amount of data. IoT platforms, such as Amazon AWS, IBM Watson or Microsoft IoT Suite, have been available to aid the development of such services/applications. However, one of the major challenges faced by IoT solutions providers is the supervision and management of the large number of deployed sensors/devices. Presumably, the magnitude and heterogeneity of the IoT systems makes it difficult to manage them with conventional IT management tools and techniques. New techniques and tools have to be explored and developed or the traditional management solutions have to be adapted to the new challenges. In this paper, we identify and formulate the essential challenges of IoT device management and supervision, review the actual state-of-the-art IoT device management and supervision techniques and tools available on the market, and briefly evaluate their features and typical use cases.**

Keywords- Internet of Things; Device Management; Platforms; Sensors.

I. INTRODUCTION

Internet of Things (IoT) enables numerous devices around the world to communicate and transfer data collected from different environments to the IoT platforms. According to Cisco, 25 - 50 billion ‘things’ will be connected to the Internet by the year 2020 [1]. This aggressive growth of emerging smart devices connected to the Internet infrastructure poses one of the most challenging tasks in the IoT space. IoT management tools need to provide solutions to meet the requirements of connectivity, heterogeneity, security, scalability and data handling [2].

The global relevance of IoT and its application to several domains, such as home and industrial automation, intelligent energy management, automotive applications, healthcare, works of life, brings in another dimension of heterogeneity as these diverse applications use a plethora of things (sensors, actuators, devices) to communicate via the Internet [3]. However, the lack of a unified approach of handling heterogeneous devices from several vendors presents a major challenge in IoT device management. Several solutions using different techniques, such as Lightweight Machine to Machine (LwM2M) [4], which manages devices remotely, have been proposed to solve these shortcomings. Unfortunately, these approaches are limited only to devices that have enough resources to implement the required management protocols and to connect directly to the Internet [5][6]. SNMP [7] and NETCONF [8] standards have also been used in monitoring IoT devices, but the heterogeneous nature often leads to waste of resources and inefficiency.

Finding an appropriate IoT management tool from the available options for a given field of application is a challenge a customer faces. Although the functionality and the performance provided by the tools are similar, their techniques and implementations are quite different. Thus, a comprehensive analysis of requirements and possible solutions is necessary to facilitate the tool selection process. In this paper, we identify and formulate the essential challenges of IoT device management and supervision, review the actual state-of-the-art IoT device management and supervision techniques and tools available on the market, and briefly evaluate their features and typical use cases.

The rest of the paper is organised as follows. Section II introduces the basics of IoT system architecture and IoT device management challenges. Section III discusses the requirements and our evaluation benchmark for comparing the management tools. The selected and investigated IoT management tools are introduced in Section IV and compared in Section V. Finally, Section VI draws the conclusions.

II. BACKGROUND

To effectively identify and evaluate the existing solutions in IoT device management, it is imperative to clearly understand the structure and challenges faced in the IoT systems. In this section, the generic architecture of IoT systems and its common challenges with regards to device management are introduced.

A. IoT System Architecture

IoT systems consist of numerous devices, such as smartphones, temperature sensors, actuators, connected in various environments. These sensors, devices, gateways are connected via communication networks to cloud services and applications. These things could be surrounded or distributed by long distances in different environments but controlled and managed centrally in the cloud, thus named cloud computing. On the other hand, a decentralized solution known as edge/fog computing is an alternative to be realized when processing is required to be carried out closer to the source of the data to improve the quality of service provided [9].

To understand the IoT system architecture, identifying and investigating its logical layering can help. In this paper, the fundamental blocks of the IoT system architecture are presented as layers and every layer forms an interesting field of research. These layers are: Sensing layer, Communication layer, Cloud layer, Management layer, and Services and Applications layer in Figure 1. The Sensing layer consists of sensors, actuators and smart devices that collect the data from surrounding environment. The Communication layer provides a means of transferring the collected data to the cloud, or the application layer. The Cloud layer aggregates the data for processing and storage, and makes it available for use to services and applications. Management data are separated from service data and collected in the management system from proper operation and administration of the entire IoT system. The Services and Applications layer presents the output data as services, applications and features offered to the end-user depending on the use-case.

The IoT communication protocols in the Communication layer and the low latency computing in the Cloud layer in addition to the provided Quality of Service (QoS) and management tools of the system determine the strengths and weaknesses of the IoT platforms and system architectures.

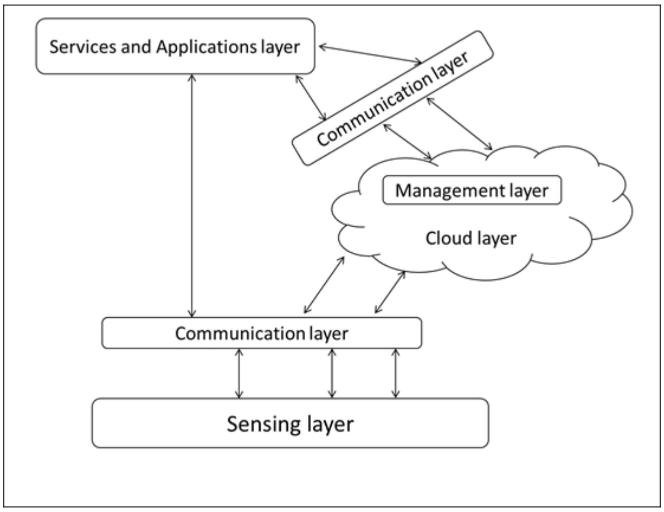

Figure 1. Layers of the IoT System Architecture.

1) Sensing layer: The main function of the Sensing layer is to detect changes in the physical status of the connected things in real-time. It includes sensors, which are the main components of this layer. The task of the sensor is to measure the physical environment, identify and localize the smart objects, collect the data and send them to the Cloud layer for processing and storage. The actuators in this layer are usually mechanical devices, such as switches, that execute the desired actions in response to changes [10].

2) Communication layer: The Communication layer is responsible for interaction between the layers of the IoT architecture. It transfers the data collected in the Sensing layer to the Cloud or the Services and Applications layer directly. It includes routers, switches and gateways, which are connected to devices that cannot connect directly to the cloud. Protocols, such as Constrained Application Protocol (CoAP) [11], Message Queuing Telemetry Transport (MQTT) [12] and Lightweight Machine to Machine (LwM2M) connect various IoT devices to send data to upper layers [13].

3) Cloud layer: It is also known as the processing unit of the IoT system. The collected data from sensors and devices are ingested in the Cloud layer. Its tasks are storing, processing, and analyzing data. In general, the cloud employs a data centre as a central server to process data generated by the edge devices. There is ongoing research on next generation cloud computing to decentralize some of the processing tasks from the cloud to edge nodes to improve computation performance [14].

4) Management layer: It is responsible for monitoring and operating all other layers, providing the features for the management tools usually implemented in the cloud.

5) Services and Applications layer: The Services and Applications layer provides the applications and a variety of the services, such as data collection, data analytics, data visualization and security. They depend on the use cases and desired functionalities provided to the end users.

B. IoT Device Management Challenges

Consequent to the accelerated evolution in IoT, service providers encounter several challenges in satisfying the management requirements. These challenges include the following ones.

1) Connectivity of Heterogeneous IoT Devices: The IoT paradigm requires widespread connectivity of billions of heterogeneous devices. This heterogenity in connectivity is considered as a significant challenge to the interoperability of protocols and solutions developed by different vendors [15]. The accessibility from anywhere can be achieved via the Internet, either by gateways or direct connection and opens the IoT system to a large environment of products and services. Moreover, remote control, which enables the management, monitoring and control of devices, is of high significance to the solutions. This will further lower operational costs by collecting data and implementing maintanance remotely [16]. The IoT system architecture is designed for use in different physical environments. Thus it requires the capability to handle many heterogeneous devices. Wherefore, a considerable concern within developing IoT solutions is handling the interaction with heterogeneous IoT devices [17].

2) Device Management Challenges: Device management is one of the most significant features expected from any IoT management tool. Retaining the device information, status and logs is important. Provision of detailed reports and information about the device level statistics is desired for numerous things [18]. As IoT devices scale to billions, the current centralized network mangement model could present bottlenecks. In an IoT system, the device integration support is required because some tasks or requirements can be done by implementing one service, while other tasks will be executed via the integration of several services [19].

3) Security Limitations: Security is a critical challenge in IoT systems because of the consequences of security breaches, such as financial and credibility losses. For instance, hackers often target the edge devices of the IoT system, which are considered as entry points [20]. Efficient IoT systems with billions of devices connected should have protection, detection mechanisms and secure procedures in case of unusual events and anticipate vulnerabilities [17]. The integration of IoT into our life extend the security concerns from information and assets to human life and health. With the rate at which technology is growing, vendors could focus more on functionality rather than security. Therefore, IoT management tools need to implement alternative techniques to handle different issues while using the identification and authentication for multiple types of IoT communication protocols used for data communication and transfer. These need to be encrypted and secured with a robust encryption algorithm to prevent possible risks [21].

4) Next Generation of IoT Management Tools: The accelerated development of IoT is impacting various scientific areas, thus inducing many trends in the next generation of IoT systems. Changing infrastructure is one of these trends because the centralized computing prototype is impressionable to single point of failures and large data centres consume huge amount of energy to keep them operating [14]. Alternate technologies being developed to reduce failures in the cloud include multi-cloud, micro cloud and cloudlet, ad hoc cloud and heterogeneous cloud [9]. In addition, minimizing the workloads for low-latency and resource processing has been a considerable challenge for cloud computing [22]. The new trend known as edge/fog computing brings processing closer to the data source [23], and the management tool is required to suit these changes and subsequently scale with the architecture and devices.

III. EVALUATION BENCHMARK

Based on the highlighted challenges, we draw a requirements/features table to serve as a benchmark for comparing the management tools reviewed in this paper (Table II). Therefore, performance and relevance of a tool have been evaluated by investigating and comparing the following requirements/features.

- *Device Management:* This is one of the most important features expected from any management tool. The tool should maintain a list of connected devices and track their operation status; it should be able to handle configuration, firmware (or any other software) updates and provide device-level error handling and reporting [18].
- *Protocols Supported:* Things require a direct communication path to the platform in both the forward and reverse direction for information exchange and sending commands. Thus, a management tool should support application and management protocols that the device can work with to exhibit a ‘device agnostic’ property. Some widely used application protocols include MQTT, CoAP, REpresentational State Transfer (REST) and eXtensible Messaging and Presence Protocol (XMPP). Other Protocols, such as LwM2M and Open Mobile Alliance - Device Management (OMA-DM) are classified as management protocols [24].
- *Product Lifecycle Management:* This involves the management of a device from installation and commissioning till its decommissioning. During the lifetime of this thing, it is necessary to make some software/firmware updates to implement new features, remove bugs and fix security vulnerabilities [25]. Thus, it is a major challenge in IoT, based on its scale of millions of devices, to individually perform these important tasks. Over-the-Air (OTA) upgrades, downgrades and option of force updates for super critical firmware are expected features of the management system.
- *Troubleshooting and Maintenance:* Diagnostics features are required in the operation of IoT devices [26]. The tool should also allow the sending of custom and system level commands to a device, such as reboot or factory reset.
- *Security and Access Control:* The security measures required for IoT systems are higher than those of general software and applications [27]. The connection of millions of devices to a network increases the vulnerabilities proportionally. Since the devices are low cost and low power, these security requirements need to be met from the platform end of the management system in the form of message-level security and data encryption [28].
- *Localisation and Mapping:* Location support is essential especially when a device’s location is not static rather dynamic. The continuous tracking of the location will thus help generate the historic location view. In some applications, GPS locations or network triangulation is necessary for fleet management and asset tracking solutions [24].
- *Scalability:* This is one of the most important non-functional features [24]. As most of the management systems are web applications, it is expected to be highly scalable to the order of millions of things. Support auto scaling feature could also be included by the application developers, so a scalability magnitude could also be defined for customers to provide some limit.
- *Device Monitoring:* Tools that can provide device monitoring and performance data visualizations are also very helpful in supervising the network of things. Alarm indications to provide alerts in case of faults and critical events should be embedded into the tool for easy and efficient monitoring of the whole network [26].
- *Integration:* Provision of standard/open APIs for integration has high importance in a management tool. As most vendors already have an existing enterprise platform, the seamless integration of a management tool via a standard API will make the operations and management much easier. The importance of the interoperability of IoT management tools cannot be over-emphasized as this is the source of a platform/device agnostic management system [28].

IV. IoT DEVICE MANAGEMENT TOOLS

In this study, we have selected a variety of tools on the market that have the potential to play an essential role in monitoring smart things in the IoT solutions. These tools were selected because they are suitable stand-alone IoT device management tools with extensive implementation in several industrial use cases. We shortly describe the selected tools in this section, while a summary highlighting their key features and example use cases is shown in Table I.

A. *Xively CPM*

Xively Connected Product Management (CPM) is a tool that offers solutions for enterprises building connected products and services. Moreover, it enables companies to easily build and manage IoT security, connected devices and products including home automation, and capturing their IoT data. It provides a simple and scalable platform enriched with tools necessary to connect, manage and engage things. It has standard APIs for integrating data with primary enterprise systems, such as Customer Relationship Management (CRM) [29][30].

B. *DevicePilot*

DevicePilot implements locating, monitoring and managing connected devices at scale. It is completely agnostic, providing platform connectivity to any device, and easily integrates with IoT platforms. It is a cloud-based application, which scales with the deployed infrastructure, schemaless and provides all functionalities via a REST API [31].

C. *Wind River HDC*

Wind River Helix Device Cloud (HDC) is a tool that helps reduce the complexities of building and managing large-scale IoT deployments. It enables device health monitoring, bi-directional file transfer, remote access to help service engineers detect and diagnose problems before they impact critical data collection. HDC provides tools one needs for deploying, monitoring, servicing, updating, and decommissioning IoT devices [32].

D. *QuickLink IoT*

QuickLink is a resource efficient device management solution based on LwM2M and OMA-DM standards. It supports device provisioning, configuration, diagnostics management and over-the-air updates. It has a plug-in API architecture with encrypted data collection using CoAP with Transport Layer Security (TLS) [33].

E. *ThingWorx Utilities*

ThingWorx Utilities is a set of tools, rich in features that enable and support the rapid deployment and adoption of powerful IoT applications. It provides device management capabilities for day to day management of the connected devices and includes utilities to provision, remotely monitor and update the connected devices and assets. With its standard framework, it is also possible to integrate new IoT applications into existing business systems [34].

F. *Particle*

Particle is a full-stack IoT device management platform that provides all the necessary tools to securely and reliably connect IoT devices to the web/cloud. The solution can be used on different scales of deployment from large enterprises to innovative start-ups and everyone in between. It is secured by using encrypted communication protocols, easy to use and provides an interface to see devices, push software updates, and make changes and improvements on an ongoing basis. It offers several development tools, such as Web IDE, Desktop IDE and a Command Line Interface (CLI). The device management console can manage team permissions from a single administrative interface. Support for cross-vendor devices is limited and continuously developed [35].

G. *Losant Helm*

Losant Helm is a fully integrated IoT device management and connectivity tool directly embedded in the Losant IoT platform, an enterprise-ready cloud platform that enables developers to easily make use of real-time data by rapidly developing smart, connected solutions for IoT. It serves as a control hub for connected production facilities and its hardware-agnostic platform is easily integrated with a broad variety of sensors, controllers, machines, and device gateways. This enables many-to-many interoperability across disparate systems and technologies. Its open communication standards (REST, MQTT) provide simple connectivity to millions of devices [36].

H. *DataV IoT Device Management*

This tool makes equipment and device management a priority as industrial companies connect more business-crucial assets together with IoT. It gives the power to manage the full lifecycle of all assets from a centralized location, including configuration, inventory, and OTA software updates and configuration [37].

V. COMPARISON OF MANAGEMENT TOOLS

Today, none of the selected and evaluated tools claims to support all the features we used in the benchmark. Interestingly, all of them support the basic features of device management, remote monitoring, product lifecycle, scalability and integration to IoT platforms. The protocols supported, localization and mapping, troubleshooting and maintenance, security and access control features are available in a limited number of these tools.

DevicePilot stands out as the star performer from this study because it supports more features than the other tools we have evaluated. Localisation of devices, access control of the connected things and support to REST protocols are its added features. Its only drawback is the lack of maintenance and troubleshooting function.

QuickLink IoT follows closely with troubleshooting and maintenance features with OTA updates added to the basic functionalities. It also supports LwM2M and OMA-DM device management protocols. It does not support mapping of devices and the security features are limited.

Particle, Losant and Wind River HDC have very good maintenance features with remote diagnostics and updates but lack localization and access control functionalities. Particle supports CoAP, MQTT and its proprietary Particle subscribe protocols. Losant integrates remote management with audit and log files from devices. HDC manages devices via MQTT protocol with security extensions.

Xively is also a very good management tool with robust security features and support to MQTT, REST and HTTP protocols. Unavailability of localization, mapping and troubleshooting and maintenance of devices are its major drawbacks.

ThingWorx Utilities and DataV both integrate well with IoT platforms. While ThingWorx supports protocols such as MQTT, CoAP and XMPP, DataV provides limited support to standard protocols. Both tools lack localization and access control features, but DataV supports troubleshooting and error log management. None of the reviewed tools fully supports all IoT-related protocols.

TABLE I. KEY FEATURES AND TYPICAL USE CASES OF THE EVALUATED IOT MANAGEMENT TOOLS

Tool	Vendor	Key Features	Typical Use Cases
XIVELY CPM [29]	LogMeIn Inc.	Device agnostic connectivity (MQTT, REST and HTTP protocols), scalability, security and IoT platform integration	Agriculture, energy management and DNA research improvement
DEVICEPILOT [31]	DevicePilot	Device management, security, scalability, mapping, real-time monitoring and easy integration	Energy management, construction, healthcare and smart cities
WIND RIVER HDC [32]	Wind River	Thing management via MQTT with security, device health monitoring, remote diagnostics and software upgrade	Smart homes, healthcare, industrial, automotive and energy management
QUICKLINK IOT [33]	SmithMicro Software	LwM2M and OMA-DM supported device management, securty, diagnostics and OTA updates	Asset management, smart monitoring, connected cars and smart cities
THINGWORX UTILITIES [34]	ThingWorx	Device management using MQTT, XMPP or CoAP, remote control and monitoring, product lifecycle and IoT platform integration	Manufacturing, healthcare, transportation and utilities
PARTICLE [35]	Particle.io	Connectivity, OTA updates, security, IoT platform integration, remote diagnostics, monitoring, reports and alerts. It supports MQTT, CoAP and Particle subscribe	Smart homes, environment monitoring, infrastructure and supply chain management
LOSANT HELM [36]	Losant	Remote provisioning, agnostic management, audits and logs, 3rd party IoT platform integration	Manufacturing, logistics and retail management
DATAV IOT DEVICE MANAGEMENT [37]	BSquare	Device health monitoring, device and error logs, real-time monitoring, performance issue resolution and IoT/enterprise platform integration	Smart metering, intelligent vending, fleet management and transportation

TABLE II. COMPARISON OF THE EVALUATED IOT MANAGEMENT TOOLS/PLATFORMS
(LEGEND: ● – SUPPORTED; ○ – NOT SUPPORTED; ◐ – PARTIALLY SUPPORTED)

Tool	Device Management	Protocols Supported	Product Lifecycle Management	Trouble-shooting and Maintenance	Security and Access Control	Localisation and Mapping	Scalability (to millions)	Device Monitoring	Integration
XIVELY	●	◐	●	○	●	○	●	●	●
DEVICE PILOT	●	◐	●	○	●	●	●	●	●
WIND RIVER HDC	●	◐	●	●	◐	○	●	●	●
QUICKLINK IOT	●	◐	●	●	◐	○	●	●	●
THINGWORX UTILITIES	●	◐	●	○	◐	○	●	●	●
PARTICLE	●	◐	●	●	◐	○	●	●	●
LOSANT HELM	●	◐	●	●	◐	○	●	●	●

DATAV IOT DEVICE MANAGEMENT	●	◐	●	●	◐	○	●	●	●

Table II compares the eight selected and evaluated IoT management tools/platforms taking into consideration that due to their continuous development some requirements will be met by the products in the nearest future.

VI. CONCLUSIONS

The current growth trends adumbrate that IoT will gain higher and higher importance in several industries in the coming years. This expands its influence on the interaction between man and technology, and the role of a functional and robust management system is getting more importance.

This paper presents the basic and fundamental requirements of an IoT management and supervision solution based on the generalized architecture of an IoT implementation. Using these requirements as a benchmark, we have selected, evaluated and compared eight industrial IoT management tools. Unfortunately, the complex structure of IoT implementations due to their numerous applications, heterogeneous devices and diverse use cases makes it challenging to come up with a generic 'one for all' management tool. However, our comparison matrix, given in Table II, can help IoT solution providers choose the most appropriate management tool for their target system assuming a good understanding of the requirements. In future, we plan to develop/extend IT management tools to meet the needs of the IoT ecosystem.

ACKNOWLEDGMENTS

The work presented in this paper has been carried out in the frame of project no. 2017-1.3.1-VKE-2017-00042, which has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the 2017-1.3. funding scheme.

This work was performed also in the frame of FIEK_16-1-2016-0007 project, implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the FIEK_16 funding scheme.

REFERENCES

[1] D. Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," CISCO IBSG, 2011.

[2] C. Pham, Y. Lim, and Y. Tan, "Management architecture for heterogeneous IoT devices in home network," 2016 IEEE 5th Glob. Conf. Consum. Electron. GCCE 2016, 2016, pp 1-5.

[3] Y. Jie, J. Y. Pei, L. Jun, G. Yun, and X. Wei, "Smart Home System Based on IoT Technologies," in 2013 International Conference on Computational and Information Sciences, 2013, pp. 1789–1791.

[4] "Lightweight machine to machine technical specification," OMA-TS-LightweightM2M-V1_0-20170208-A, Open Mobile Alliance, Feb 2017.

[5] S. Rao, D. Chendanda, C. Deshpande, and V. Lakkundi, "Implementing LWM2M in constrained IoT devices," in 2015 IEEE Conference on Wireless Sensors (ICWiSe), 2015, pp. 52–57.

[6] M. Ersue, D. Romascanu, and J. Schoenwaelder, "Management of Networks with Constrained Devices: Problem Statement and Requirements," RFC 7547, May 2015

[7] D. Harrington, R. Preshun, and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks," RFC 3411, December 2002.

[8] R. Enns, M. Bjorklund, and A. Bierman, "Network Configuration Protocol (NETCONF)," RFC 6241, June 2011.

[9] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick and D. S. Nikolopoulos, "Challenges and Opportunities in Edge Computing," 2016 IEEE International Conference on Smart Cloud (SmartCloud)," New York, NY, 2016, pp. 20-26.

[10] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Commun. Surv. Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

[11] J. Guth, U. Breitenbücher, M. Falkenthal, F. Leymann, and L. Reinfurt, "Comparison of IoT platform architectures: A field study based on a reference architecture," 2016 Cloudification of the Internet of Things (CIoT), 2016, pp. 1-6.

[12] C. Bormann et al, "CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets," RFC 8323, 2018.

[13] OASIS.org, "MQTT version 3.1.1," OASIS Standard, October 2014, http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html, [retrieved: June 2018].

[14] B. Varghese, and R. Buyya, "Next Generation Cloud Computing: New Trends and Research Directions," Future Generation Computer Systems, 2017, pp. 1–22.

[15] M. Elkhodr, S. Shahrestani, and H. Cheung, "The Internet of Things : New Interoperability, Management and Security Challenges," International Journal of Network Security & Its Applications, vol. 8, 2016, pp. 82-102.

[16] "Remote Monitoring and Maintenance: Mission-Critical Operations at the Competitive Edge," Oracle, 2016, [Online], Available: http://www.oracle.com/us/solutions/internetofthings/iot-remote-monitoring-brief-2881653.pdf, [retrieved: May, 2018].

[17] T. Perumal, S. K. Datta, and C. Bonnet, "IoT device management framework for smart home scenarios," 2015 IEEE 4th Glob. Conf. Consum. Electron. GCCE 2015, 2016, pp. 54–55.

[18] V. Gazis et al., "A survey of technologies for the Internet of Things, 11th International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, 2015, pp. 1090-1095.doi: 10.1109/IWCMC.2015.7289234.

[19] J. Lin et al., "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," IEEE Internet of Things Journal, vol. 4, no. 5, 2017 pp. 1125–1142. doi: 10.1109/JIOT.2017.2683200.

[20] K. Shea, "Device Management in the Internet of Things – Why It Matters and How to Achieve It," WindRiver, 2017, [Online] Available: http://www.new-techeurope.com/2017/06/07/device-management-internet-things-matters-achieve/, [retrieved: May 2018].

[21] Jasper (2014), "Achieving End-to-End Security in the Internet of

Things," [online], Availabe: http://pages.jasper.com/White-Paper-Cellular-IoT-Security_Cellular-IoT-Security.html, [retrieved: May 2018].

[22] P. Varshney and Y. Simmhan, "Demystifying Fog Computing: Characterizing Architectures, Applications and Abstractions," Proc. - 2017 IEEE 1st Int. Conf. Fog Edge Comput. ICFEC 2017, 2017, pp. 115–124.

[23] D. C. Klonoff, "Fog Computing and Edge Computing Architectures for Processing Data from Diabetes Devices Connected to the Medical Internet of Things," J. Diabetes Sci. Technol., vol. 11, no. 4, 2017, pp. 647–652.

[24] P. Ganguly, "Selecting the right IoT cloud platform," 2016 International Conference on Internet of Things and Applications (IOTA), Pune, 2016, pp. 316-320. doi: 10.1109/IOTA.2016.7562744.

[25] B. Moran, M. Meriac, H. Tschofenig, "IoT Firmware Update Architecture," IETF Internet-Draft, [online], Available: https://tools.ietf.org/html/draft-moran-suit-architecture-00, [retrieved: May 2018].

[26] "Internet of Things will require remote monitoring solutions", Opengear, [online], Available: https://opengear.com/articles/internet-things-will-require-remote-monitoring-solutions-order-succeed, [retrieved: May 2018]

[27] L. Atzori, A. Iera, G. Morabito, "The Internet of Things: A survey," Computer networks, 54(15), 2010, pp.2787-2805.

[28] "What makes device management a core compatibility of an IoT platform," Softweb Solutions, [online], Available: https://www.softwebsolutions.com/resources/IoT-device-management-platform.html, [retrieved: May 2018].

[29] "Connected Product Management," Xively, [online], Available: https://www.xively.com/xively-iot-platform/connected-product-management, [retrieved: May 2018].

[30] "Guide to Connected Product Management (CPM)," Xively, [online], Available: https://www.xively.com/resources/guide-to-connected-product-management, [retrieved: May 2018].

[31] "Device Pilot Features," Device Pilot, [online], Available: https://www.devicepilot.com/about/features/, [retrieved: May 2018].

[32] "Wind River Helix Device Cloud," Wind River, [online], Available: https://www.windriver.com/products/helix/device-cloud/, [retrieved: May 2018].

[33] "Overview of QuickLink IoT Services Platform," SmithMicro Software, [online], Available: https://www.smithmicro.com/iot-oem/products/quicklink-iot-services-platform/overview, [retrieved: May 2018].

[34] "Manage Your Industrial IoT with ThingWorx," ThingWorx [online], Available: https://www.ptc.com/en/products/iot/thingworx-platform/manage, [retrieved: May 2018].

[35] "Device Cloud," Particle, [online], Available: https://www.particle.io/products/software/device-cloud, [retrieved: May 2018].

[36] "Data and Device Management," Losant, [online], Available: https://www.losant.com/iot-platform/data-and-device-management, [retrieved: May 2018].

[37] "DataV IoT Device Management, BSquare, [online]. Available: https://www.bsquare.com/iot-device-management/, [retrieved: May 2018].