Survey of Platforms for Massive IoT

Hamdan Hejazi
Department of Automation and Applied Informatics
Budapest University of Technology and Economics
Budapest, Hungary
eng.hamdano@hotmail.com

Husam Rajab
Department of Telecommunications and Media Informatics
Budapest University of Technology and Economics
Budapest, Hungary
husamrajab@tmit.bme.hu

Tibor Cinkler
Department of Telecommunications and Media Informatics
Budapest University of Technology and Economics
Budapest, Hungary
cinkler@tmit.bme.hu

Laszlo Lengyel
Department of Automation and Applied Informatics
Budapest University of Technology and Economics
Budapest, Hungary
lengyel@aut.bme.hu

Abstract*— Internet of things (IoT) becomes a prominent technology in our world. It is enabling the connection between the objects (the "things") and the backend systems via the Internet. Everyday objects can become connected and smart. It has been adopted in different areas and applications such as smart cities, smart agriculture, smart healthcare, smart manufacturing, and others. Moreover, IoT platforms are currently growing up into the market. Each platform provides valuable and specific services and features. This paper presents a survey on IoT platforms, discussing their architectures and fundamentals of IoT building elements and communication protocols between them. The aim of this paper is to help the reader choose a suitable and adequate IoT platform for own demands in the huge number and variety of platforms available. This survey provides a comprehensive view of the components and features of the state-of-the-art IoT platforms.

Keywords—Internet, IoT, Massive IoT, Platforms, Protocols, M2M, LW M2M, CoAP, NB-IoT, LoRa, LPWAN

I. INTRODUCTION

The Future Internet enables us to have an immediate access to the information of the physical world and its objects. As such, Internet of Things (IoT) has been adopted to incorporate the digital information and the real world of devices. The things we use have the ability to connect to the Internet, for instance, watches, TVs, vehicles, machines and more. The accelerated growth of IoT industry requires robust IoT platforms which address the renewal requirements such as in the smart cities applications, an enormous amount of data has to be handled.

Internet of Things can be presented as a network of surrounding things which are connecting to internet such as various sensors, vehicles, devices which can be monitored, detected, controlled. The things are embedded with the sensors to sense the environment and communicate with other things [1]. The environment is monitored and the things have the ability to sense, to be identified uniquely, and to perform any predefined action. Users can access the things through the internet and get notified and take action to control the environment.

IoT platforms provide varied capabilities in the Industry. Emerging industrial IoT and the fourth industrial revolution (Industry 4.0) provides the flexibility for the planners and implementers and leads to better decision-making. Moreover, the machine monitoring and the cloud services in addition to provided applications contribute to growth and production.

Finding an appropriate IoT platform for a given field of application is a challenge any company is facing when wanting to select the appropriate platform from the mess of different IoT platforms. Although the functionality provided by IoT platforms is similar or even equal, their implementation and the underlying technologies difference. Sometimes, platform selection process is done without a detailed analysis of requirements [2].

Current IoT platforms have a market share and offer for the customers some competitive advantages and features to make them select it and encourage their choice. It provides several services and applications such as data acquisition and analytics, device management, integration, security, insight to users on the operations and ability to identify and manage devices. There are different IoT models such as on-premise model which is operated on the same premises or organizations and platform as a service which is off-premises and uses typically cloud computing. The companies often select based on these models.

The rest of the paper is organised as follows. Section II introduces Comprehension of IoT Platform Parts. Section III discusses IoT Communication Protocols and the main purpose for using IoT protocols. Next, we list the main roles of IoT platforms in Section IV. Section V provides hints on choosing the platform for certain needs. In Section VI, we present the results of our survey on a selection of IoT Platforms for massive IoT applications. The survey ends with concluding remarks on the proposed use of IoT platforms in Section VII.

II. COMPREHENSION OF IOT PLATFORM PARTS

A. The "Concept" of an IoT platform

IoT platforms consist of a huge number of objects connected together around the world. It connects the edge of devices, gateways, and data networks to cloud services and applications. The objects could be surrounded or separated by long distances in different environments but controlled by the centralized management that plays the role of the processing unit of the IoT platform. To understand the behavior of IoT platforms, there is a need to investigate and identify the elements / components / blocks to more comprehend IoT

attitude and veritable sense. In this paper, the essential blocks of IoT platforms are presented as components because every block of IoT platforms becomes an attractive field of research, they make a loosely coupled system and all the blocks are influential in the competition between IoT vendors. The components consist of: sensing component, communication and identification component, computation and cloud component and finally services and applications component. The IoT protocols within the communication and identification component, and the average of processing speed in computation and cloud part in addition to featured services and application provided determine the strengths and weaknesses in all the platforms. A massive survey of platforms for massive IoT has been accomplished in this paper by including different aspects of comparison of IoT platforms.

Internet of Things platforms is a remarkable topic in the technological industry. Most of the studies and researches in the literature concentrate on presenting the IoT approaches. Standardization in IoT signifies to the importance of improving the interoperability between different applications, services and users. Moreover, Web of Things (WoT) is correlated with the IoT [3], through in web world, data visualization and applications provided to users are based on IoT platforms. The majority of IoT platforms has some web browser-based graphical frontend for human communication with, and human control of things connected via the Internet.

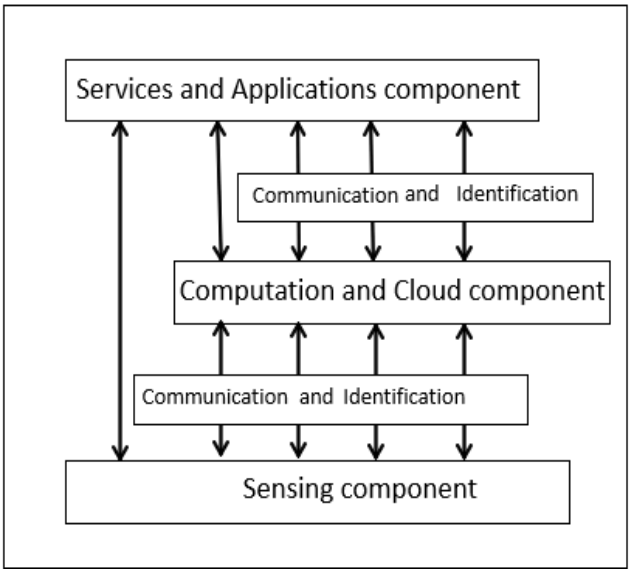
B. Components of an IoT Platform

The functionality of IoT as described in [4] [5] consists of six blocks: (1) Identification block which means each IoT object must be uniquely defined such as with an assigned unique ID within the network of the objects; (2) Sensing block for sensing the environment; (3) Communication block that defines the IoT communication technologies; (4) Computation block responsible for processing and computational ability of the IoT; (5) Services block representing all the categories of services provided by IoT platforms and (6) Semantics block that provides examples of web technology on how to extract information and deal smartly with the diverse machines to provide the desired services. Zheng et al [6] drive a three-layer architecture including similar concepts to those summarized in our reference architecture.

In this paper, we represent IoT reference platform as a simpler four-part architecture as shown in Figure 1: (1) sensing component which include sensors, actuators and devices, (2) a communication and identification component represents the communication protocols (and a gateway if needed), (3) a computation and cloud component represent the tasks of "processing unit" of IoT and finally (4) the services and applications component that represents the provided services and features offered to the user to connect and to control the environment through the IoT platform. There might be direct communication between "sensing component" and "services and applications component" without the computation and cloud component. However, then we have no IoT platform in strict sense.

a. Sensing component:

One of the main objects in IoT platform is the sensor which detects the physical environmental condition. The task of the sensor is measuring the parameters and sensing the physical environment then converting them into an electrical signal. It collects accurate sensory data from IoT objects and transfers it to a specific destination such as a database with data management or it is analyzed through cloud computing.



Actuators are hardware mechanical devices such as switches that undertake the requested response to changes. They produce and convert electrical signals into physical actions. The device is represented by any hardware component connected either by wires or wirelessly to handle data from sensors and to control actuators.

Figure 1: Components of an IoT Platform

b. Communication and Identification component

IoT objects in need of communication jointly with the upper system to handle collected data., a gateway which is connected to devices and it uses in state of a device not eligible to direct connection with other systems. For instance, the gateway is used when the device not able to communicate via a specified protocol. It supports the IoT communication protocols in send and receives data. Communication component contains IoT communication protocols such as CoAP and MQTT to connect various IoT objects to send data to management system [2]. The identification in addition to authentication provides significant performance gains in networks and operations of sensors, actuators and devices. It assists in the detection of returned faults of the processes. Each object acquires uniqueness by unique identifiers by certain identification technologies. Sensors and devices connected over internet by an adequate communication technology, such as Wi-Fi, RFID, LTE, etc.

c. Computation and Cloud component:

Today's IoT platforms are typically cloud-based. There are various technologies and processes. Data from sensors and devices is collected and processed in a cloud of the IoT platform. This component can be named as IoT integration

middleware because this component represents the processing unit and provides the computational capability of the IoT it serves as an integration layer for different kinds of sensors, actuators, devices and applications. It supports suitable communication technologies, transport protocols such as WebSockets to communicate with devices, as well as between platforms. Corresponding payload format, such as JSON or XML is used for messages.

d. Services and Applications component:

A verity services provided by IoT platforms such as data collection and data analytics, support for data visualizations, management, incorporation, security. Connectivity is provided as a service by empowering the free access to devices. Analytical tools can be used in the application development, based on data collected by the sensors and devices.

III. IoT PROTOCOLS

The huge number of connected objects or devices produce machine-to-machine M2M systems. It is a type of IoT system and the other part of the system need to be configured, maintained, monitored and support the services and device management in their lifetime. Lightweight machine-to-machine M2M is protocol from the Open Mobile Alliance which is an open industry protocol, it assists in implementing service and application management remotely for IoT connected devices. Lightweight M2M is a communication protocol for communication operations between M2M devices such as client software and M2M management and service enablement platform which is contained in server software. A standard review for Lightweight M2M (LwM2M 1.0) specifications is given in [7]. Machina Research [8] expects that M2M connections will raise to 12 billion in 2020. There are a lot of features for Lightweight M2M such as it is based on efficient and secure IETF standards, for instance, Constrained Application Protocol (CoAP) and Datagram Transport Layer Security (DTLS), interfaces include bootstrapping, registration, management and services, and services reporting. Also, building object model (the so-called smart objects) and efficient payloads [9]. Finally, different communication technologies are used between devices and the platform, within the platform and between the platform and the users. Also, there is a large variety of communication solutions between the IoT module and the platforms such as LoRa, NB-IoT, ZigBee.

A. CoAP

Constrained Application Protocol, It is a new communication protocol that specifically designed for hardware inspired by Hypertext Transfer Protocol (HTTP) and uses one to one communication. CoAP used for hardware does not support TCP/IP communication and need low energy. It uses User Datagram Protocol (UDP) and IP and more efficient protocol than HTTP or Representational State Transfer (REST) API, etc. It uses fewer resources than HTTP and implements more features than HTTP such as observe and discover features. A performance comparison between HTTP and CoAP is inspected for energy consumption and response time in [10]. Observe mean that the server or another device will observe that there is a change in the state and notify about that. Discover feature included in CoAP to find out devices that are in the surrounding environment., Moreover, a typical IoT platform could propose a variety of standardized communication protocols where the device manufacturer may choose the suitable protocols.

B. MQTT

Message Queue Telemetry Transport (MQTT) is a messaging protocol implemented over TCP/IP a published subscribe lightweight communication protocol. It uses message broker server in the middle in communication between devices. So, it is not a machine to machine communication. It consists of three elements, subscriber, publisher and broker. Then the clients publishing and subscribing to topics on the broker. For instance, if there are three clients and two clients of them subscribe to the same topic, e.g. temperature. Then the third client will publish to the same topic that the temperature is 30 degree, while the other clients will receive notification on that temperature. In terms of security, MQTT supports Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

CoAP versus MQTT

There is always question what is the best IoT protocol? The answer depends on which type of application of IoT used. In WAN network case, MQTT is better due to the concept of the broker. The broker is the middle in communication between devices. It will be useful in limited bandwidth such as remote different sites or lacking networks. For instance, Amazon service and Azure use MQTT protocol [7].

CoAP is compatible with HTTP. For web services-based, CoAP is a good choice for them. It can use in case of using less bandwidth and local networks because CoAP uses UDP (User Datagram Protocol) that has support for multicast and broadcast. It is used where devices need to transmit and receive at high speed. Also, it depends on the type of application, for instance, if there are a few UDP messages need to send, the CoAP will be better to use instead of the Transmission Control Protocol (TCP) based MQTT.

IV. WHY WE USE THE IoT PLATFORMS

IoT is collective types of technology, it's an aggregation of sensors, devices, networks, and software that works together to release the valuable and effective data from the Internet of things. What brings those components to implement together in IoT platform, and selecting the specific platform for your business is necessary to the success of your solutions in the present and future.

IoT is not a single technology, it's an aggregation of sensors, devices, networks, and software that works together to unlock the valuable and effective data from the Internet of things. A platform will orchestrate many of the fundamental aspects that go into making an IoT solution work. These include determining how a particular endpoint connects to a network, how and where data is collected, and finally, how that data can be used to drive business value. Therefore, the main purpose for using IoT platforms are: First, IoT networks and multi-network connectivity. Recently, various types of network technology options were used to link IoT devices, however, the

best choice of the networking solution depends on how and where it will be used, as long as the required service level is guaranteed. For this reason, an inclusive IoT platform should support the connectivity and provide all major IoT types to show the greatest flexibility for recent and future projects.

Secondly, IoT service management, using an IoT platform is an important point to get better managing of your own work and business and also to improve the efficiency, and optimize operations. For keep the IoT solutions continuously working, it is important to manage the data and IoT networking simultaneously. IoT platforms should provide administration for accessing the user-controlled software tools to keep managing the devices and the connections via the networks as an aspect of IoT solution. Also, an appropriate on-demand service management implementation allows the control of the IoT network, providing adding, moving, removing, or changing IoT device reporting functions. IoT devices and applications could be managed in an effective way for enhancing the IoT deployments [20].

Thirdly, IoT data management and application enablement, Orchestrating data. Most of IoT solutions leverage various of sensors that can generate a high volume of data over time, such as: location, condition, and status. The information is collected and stored as data streams. Each data point is usually short, while the amount of information collected rapidly, relying on the reporting frequency of IoT devices. An IoT platform supports the ability to secure and normalize the information from diverse various of IoT endpoints, practically any device and any sensor reading. Multiple devices sending streams of information and after receiving information could break them down, so the received information can be easily processed, used, or reacted depending on the information received through applying the commands.

Fourthly, Analytics, Statistic processing and data management by various data connections and hardware have to make a result about accurate data analytic. the ultimate goal of data gathering is to fuel better business outcomes through increased visibility and insight. An IoT platforms could provide complete information and view of data analytics capabilities that can extract the information and remain business from shipwright of new information that might be weakly organized. This will cover analysis performed on an IoT platform, as well as the ability to leverage specialized third-party analytics software via secure API and services.

Finally, Security with multiple layers, one of the main major to be concern for any business in IoT is security. For low-level protocols including security and privacy for both centralized and distributed IoT description in the survey [21]. Following essence security rules and practices will decrease the risks and increase the benefits of leveraging new sorts of connected devices.

V. WHAT'S THE ROLE OF AN IOT PLATFORM?

IoT platforms play important role in many aspects of our life. It is considered to be the "backbone" of the smart cities, the mean of monitoring the surrounding environment (e.g., weather, temperature, humidity), the intelligence of transportation systems including smart parking places. The clouds collect the data and store it in a distributed database to perform filtering, analysis, computation, decision, management, translation and visualisation of data as end application service.

IoT platforms provide connectivity service as component of IoT platform and there are special connectivity platforms that connect between the customers and their devices such as SIGFOX1 which a provider of low-power and long-range connectivity, HOLOGRAM2 which is a cellular connectivity platform provides inexpensive SIMs and CISCO JASPER3 which was acquired by Cisco in 2016, is a cellular connectivity management platform [8]. Security in IoT platforms means providing a secure connection of devices, transfer trusted data to handle in the cloud and keep continued valuable value through analytics. Additional functions required include providing functions such as authentication, authorization, content integrity, and data security. Moreover, [9] reviews briefly the challenges and problems of IoT coordination, for example, IoT interoperability, context awareness, and discovery.

VI. SELECTING THE RIGHT IOT PLATFORM

The most difficult question for a company is how to select the suitable IoT platform form a huge offer of different IoT platforms of different vendors and different providers. Each provider has specific features and different services distinguishing it from the others. The consideration depends on several factors such as hardware type, protocols, data visualization, the required service, etc. So, the company must investigate these options before considering to invest into a certain IoT platform [10].

- The stability of the platform: Throughout plenty of platforms in the market, it's a possibility some will fail. It's important to choose a platform that's probably to be around for several years, furthermore, your investment might be waste if the platform provider fold. And to be sure the chosen platform is good or not, ask about the current and past customers.
- The scalability and flexibility of the platform: Make sure that the platform works when you're small and just beginning because with times your needs will be changing with time. However, it will also work when you're growing fast. As well as to being scalable, the platform should be flexible enough to keep up with rapidly changing protocols, technologies, or features. It's also important that the platform is network agnostic. This means that it can integrate and work with all major tech systems out there, rather than be locked into one vendor.
- The pricing model and business case: a platform providers is an explicit in their pricing, some will show a prefatory rate and after that rise it up significantly when the contract being to sign up. In the pre-IoT product days, manufacturing costs were a lot more straight-forward: materials, fabrication, distribution. Now in the days of IoT new cost considerations must be made: network, servers, cloud, etc. This is a tough

riddle to solve because these new costs are inherently subscriptions (operational expense) as opposed to one-time upfront fees (capital expense).

VII. Review of today's IoT platforms

Recently there are more than 300 IoT platforms [11] [12][13]in the market today, and it's rapidly growing. However, the discussed Platforms in the schedule not the same, IoT platforms are being shaped by varying entry strategies of different companies trying to capitalize on the IoT potential. Mobility management companies, Innovation startups, hardware, security and network equipment are all competing to become the best IoT platform in the market. It's oblivious from the table below, that few IoT platforms fully support device control management capabilities.

Moreover, there's comparatively a little support for analyses the generated IoT information in terms of both visualization and computation. Most of IoT platforms listed support real-time analytics, that is a must in any IoT framework. On other hand visual interface of data via graphical frontends, mostly focused on simple patterns of web portal. Those panels provide authorization to manage IoT ecosystem, however, few support the ability of visual data analytics.

There are a few characteristics that are generally noticed throughout different IoT platforms. E.g., they contain REST API based integration, they provide MQTT protocol as a means of data aggregation, also connect encryption using (Secure Sockets Layer) SSL, Transport Layer Security (TLS), Datagram Transport Layer Security (DTLS). Meanwhile not mentioning the scalability in the table. Through designing stage for IoT platforms are not indicates much consideration for the system performance aspects of an IoT deployment.

Through this section, we survey some of the available IoT platforms of both types, proprietary and open-source, that link smart objects or things to the Internet. The table lists 20 selected IoT platforms compared in our survey, arranged alphabetically. The table of the listed surveyed platforms ought to be seen in details though we suppose that an available sample of platforms is represented and included in the survey.

Schedule of surveyed IoT platforms and summarize some features which are seen by the authors as essential for matching their anticipation of the users and application developers. In Table 1 below lists the surveyed platforms. Information is provided for helping selection of the most proper IoT platform.

Open-source platforms are considered to be more promising when comparing to proprietary alternatives for the following reasons. Firstly, using open source is predicted to become faster combination of new IoT solutions towards the applications scope. Secondly, using open source has been declared to speed up the adoption of a software technology in bottom-up process. Finally, from social perspective excessive, the industry based on open source platforms to support larger welfare, compared with industry structures based on proprietary platforms [14].

However, just only a few platforms do not have a REST API. This observation predicts that the existing IoT services will tend to become closer to conventional web services (i.e., Web of Things [15]). Certainly, IoT service mashups and data analysis will be merging the key for the future of IoT technologies [16][17][18]. We indicate that only a few of platforms have combined some sort of service discovery techniques even in a very simple type. A comprehensive survey constrained M2M communication protocols can be found in [19].

VIII. Conclusions

The idea of the Internet of Things is emerging rapidly on finding out their route to our modern life, aiming to enhance the finesses of the life by linking many smart devices, technologies, and applications together. This paper has provided an overview of IoT architecture and their features, and the recent research addressing different aspects of the IoT. The investigation covers many aspects such as device management, integration, security, protocols for data collection, types of analytics, support for visualizations. This, in turn, could expand the foundation of understanding the architecture and the role of different components and protocols that framing the IoT. Particularly to the description in Section III Our architecture represented in new design.

Future works could present a detailed comparison and description of could platforms, Standardized Protocols for the Internet of Things and the types of IoT platforms.

IoT Software Platform	Device management?	Integration	Security	Protocols for data collection	Types of analytics	Support for visualizations?
AirVantage	Yes (Needs gateway)	REST API	*Unknown	MQTT, CoAP	Real-time analytics	Yes (User Interface Integrator)
Appcelerator	No	REST API	Link Encryption (SSL, IPsec, AES-256)	MQTT, HTTP	Real-time analytics (Titanium [1])	Yes (Titanium UI Dashboard
AWS IoT platform	Yes	REST API	Link Encryption (TLS), Authentication (SigV4, X.509)	MQTT, HTTP1.1	Real-time analytics (Rules Engine, Amazon Kinesis, AWS Lambda)	Yes (AWS IoT Dashboard)
Bosch IoT Suite - MDM IoT Platform	Yes	REST API	*Unknown	MQTT, CoAP, AMQP, STOMP	*Unknown	Yes (User Interface Integrator)
Carriots	Yes	REST API	Unknown	MQTT	Real-time analytics	Yes (User Interface Integrator)
Ericsson Device Connection Platform (DCP) - MDM IoT Platform	Yes	REST API	Link Encryption (SSL/TSL), Authentication (SIM based)	CoAP	*Unknown	No
EVRYTHNG - IoT Smart Products Platform	No	REST API	Link Encryption (SSL)	MQTT, CoAP, WebSockets	Real-time analytics (Rules Engine)	Yes (EVRYTHNG IoT Dashboard)
Eurotech Device Cloud	Yes	REST API	Unknown	MQTT	Real-time analytics	Yes (Everyware™ Software Framework)
Exosite	Yes	REST API	Link Encryption (SSL)	CoAP, WebSocket	Real-time analytics	Yes (Web portal)
IBM IoT Foundation Device Cloud	Yes	REST and Real-time APIs	Link Encryption (TLS), Authentication (IBM Cloud SSO), Identity management (LDAP)	MQTT, HTTPS	Real-time analytics (IBM IoT Real-Time Insights)	Yes (Web portal)
Intel® IoT Platform	Yes	REST and Real-time APIs	Unknown	MQTT	*Unknown	Yes (Web portal)
Lelylan	Yes	REST API	Link Encryption (SSL/TSL), Authentication (SIM based)	MQTT, WebSocket	Real-time analytics	Yes (Web portal)"Apache License, Version 2.0"

IoT Software Platform	Device management?	Integration	Security	Protocols for data collection	Types of analytics	Support for visualizations?
Microsoft Azure IoT Suite	Yes	REST API	Link Encryption (SSL/TSL),	HTTP, AMQP, MQTT	Real-time analytics	Yes (Web Portal)
Litmus Loop	Yes	REST API	*Unknown	MQTT	Real-time analytics	Yes (Web portal)
ParStream - IoT Analytics Platform***	No	R, UDX API	*Unknown	MQTT	Real-time analytics, Batch analytics (ParStream DB)	Yes (ParStream Management Console)
PLAT.ONE - end-to-end IoT and M2M application platform	Yes	REST API	Link Encryption (SSL), Identity Management (LDAP)	MQTT, SNMP	*Unknown	Yes (Management Console for application enablement, data management, and device management)
Samsung ARTIK Cloud	Yes	REST API	Link Encryption (SSL)	LWM2M, CoAP, MQTT, IPv6	Real-time analytics	Yes (Web portal)
Temboo	Yes	REST API	*Unknown	MQTT, CoAP	Real-time analytics	Yes (Web portal)
ThingWorx - MDM IoT Platform	Yes	REST API	Standards (ISO 27001), Identity Management (LDAP)	MQTT, AMQP, XMPP, CoAP, DDS, WebSockets	Predictive analytics (ThingWorx Machine Learning), Real-time analytics (ParStream DB)	Yes (ThingWorx SQUEAL
Xively- PaaS enterprise IoT platform	No	REST API	Link Encryption (SSL/TSL)	HTTP, HTTPS, Sockets/ Websocket, MQTT	*Unknown	Yes (Management console)

Table 1: Comparison of IoT Platform

REFERENCES

[1] M. Sruthi and B. R. Kavitha, "a Survey on Iot Platform," vol. I, no. I, pp. 468–473, 2016.

[2] J. Guth *et al.*, "Comparison of IoT Platform Architectures : A Field Study based on a Reference Architecture Comparison of IoT Platform Architectures : A Field Study based on a Reference Architecture," pp. 1–6, 2016.

[3] V. Trifa and D. Guinard, "Towards the Web of Things," pp. 1–4, 2009.

[4] S. Agrawal and D. Vieira, "A survey on Internet of Things - DOI 10.5752/P.2316-9451.2013v1n2p78," *Abakós*, vol. 1, no. 2, 2013.

[5] 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.

[6] L. Zheng, H. Zhang, W. Han, and X. Zhou, "Technologies, applications, and governance in the Internet of Things," *Proc. Internet things-Global Technol. Soc. trends*, pp. 141–175, 2011.

[7] Open Mobile Alliance, "Enabler Validation Plan for Lightweight M2M," pp. 1–16, 2014.

[8] Alliance Open Mobile, "Lightweight Machine to Machine

Requirements," pp. 1–112, 2012.

[9] A. Capossele, V. Cervo, G. De Cicco, and C. Petrioli, "Security as a CoAP resource: An optimized DTLS implementation for the IoT," in *IEEE International Conference on Communications*, 2015, vol. 2015–Septe, pp. 549–554.

[10] W. Colitti, K. Steenhaut, N. De Caro, B. Buta, and V. Dobrota, "Evaluation of constrained application protocol for wireless sensor networks," in *IEEE Workshop on Local and Metropolitan Area Networks*, 2011, pp. 1–6.

[11] Jonathan Fries, "Why are IoT developers confused by MQTT and CoAP? - IoT Agenda," 2017. [Online]. Available: http://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Why-are-IoT-developers-confused-by-MQTT-and-CoAP. [Accessed: 10-Oct-2017].

[12] Brandon Cannaday, "Top 3 Connectivity Platforms For Your IoT Devices | Losant Enterprise IoT Platform." [Online]. Available: https://www.losant.com/blog/top-3-connectivity-platforms-for-your-iot-devices. [Accessed: 12-Oct-2017].

[13] S. Agrawal and D. Vieira, "A survey on Internet of Things - DOI 10.5752/P.2316-9451.2013v1n2p78," *Abakós*, vol. 1, no. 2, pp. 1–6, Nov. 2013.

[14] LinkLabs, "IoT Platforms: What They Are & How To Select One," *August 03, 2016*, 2016. [Online]. Available: https://www.link-labs.com/blog/what-is-an-iot-platform. [Accessed: 22-Oct-2017].

[15] N. Economides and E. Katsamakas, "Two-Sided Competition of Proprietary vs. Open Source Technology Platforms and the Implications for the Software Industry," *Manage. Sci.*, vol. 52, no. 7, pp. 1057–1071, 2006.

[16] J. L. Pérez, Á. Villalba, I. Larizgoitia, and V. Trifa, "The COMPOSE API for the Internet of Things," *World Wide Web*, pp. 971–976, 2014.

[17] C. W. Tsai, C. F. Lai, M. C. Chiang, and L. T. Yang, "Data mining for internet of things: A survey," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 77–97, 2014.

[18] X. Qin and Y. Gu, "Data fusion in the Internet of things," in *Procedia Engineering*, 2011, vol. 15, pp. 3023–3026.

[19] M. Ma, P. Wang, and C.-H. Chu, "Data Management for Internet of Things: Challenges, Approaches and Opportunities," in *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, 2013, pp. 1144–1151.

[20] P. K. Verma *et al.*, "Machine-to-Machine (M2M) communications: A survey," *Journal of Network and Computer Applications*, vol. 66, no. C. Academic Press Ltd., pp. 83–105, May-2016.

[21] M. A. Rajan, P. Balamuralidhar, K. P. Chethan, and M. Swarnahpriyaah, "A Self-Reconfigurable Sensor Network Management System for Internet of Things Paradigm," *2011 Int. Conf. Devices Commun.*, pp. 1–5, Feb. 2011.

[22] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Comput. Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.