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

László 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 in 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. This paper aims 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 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 can 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 the 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 can 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 various 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 are different. 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 cloud computing typically. 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 primary purpose for using IoT protocols. Next, we list the leading roles of IoT platforms in Section IV. Section V provides hints on choosing the platform for particular needs. In Section VI, we present the results of our survey on a selection of IoT Platforms for large 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 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 behaviour of IoT platforms, there is a need to investigate and identify the elements/ components/blocks to more comprehend IoT attitude and absolute sense. In this paper, the essential blocks of IoT platforms are presented as components because every block of

978-1-5386-1208-8/18/$31.00 ©2018 IEEE

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 of 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 info-communication technology (ICT) industry. Most of the studies and researchers in the literature concentrate on presenting the IoT approaches. Standardization in IoT signifies 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 have 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, including actuators, that act when required; (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 the strict sense.

a. Sensing component:

One of the principal 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 also used in IoT platforms such as switches that undertake the requested response to changes. They produce and convert electrical signals into physical actions. It operates in the opposite way of a sensor. The device is represented by any hardware component connected either by wires or wirelessly to handle data from sensors and to control actuators.

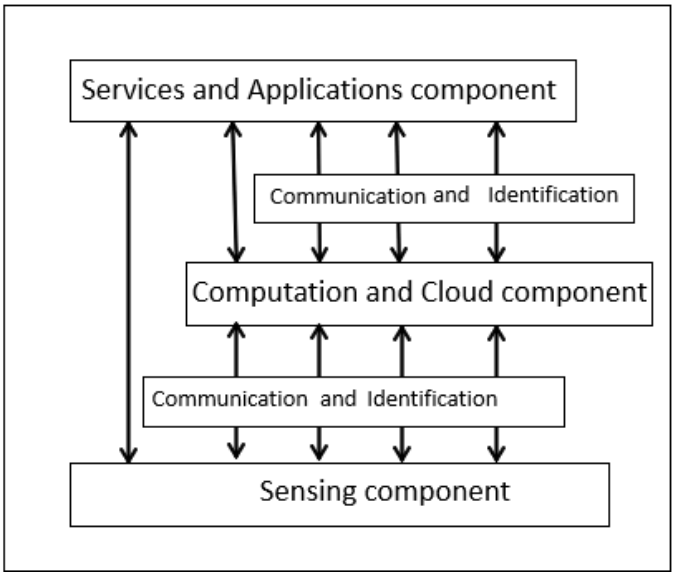

Figure 1: Components of an IoT Platform

b. Communication and Identification component

IoT objects in need of communication jointly with the upper system 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 is not able to communicate via a specified protocol. It supports the IoT communication protocols in sending and receiving data. We must emphasize that in real-IoT systems the whole IP protocol stack is implemented on the end devices. Although it will load the end device, it will make "gateway-less" end-to-end communication possible. The 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 specific identification technologies. Sensors and devices connected to the Internet by an adequate communication technology, such as Wi-Fi, ZigBee, NFC, BLE, LTE, LoRa, SigFox or NB-IoT.

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 that is part 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 combination layer for different types 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 variety of the services provided by IoT platforms include 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 massive number of connected objects or devices of the Internet produce machine-to-machine M2M systems. It is a type of the IoT system and the other part of the system needs to be configured, maintained, monitored and must support the service and device management in their lifetime. Lightweight machine-to-machine M2M protocol from the Open Mobile Alliance 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 rise to 12 billion in 2020. There are many 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 or other.

A. Constrained Application Protocol (CoAP)

Constrained Application Protocol (CoAP), is a new communication protocol that is designed explicitly for IoT hardware that is inspired by the Hypertext Transfer Protocol (HTTP) and uses one-to-one communication. Since CoAP is used for IoT hardware has to be lightweight, thin, and to generate as little traffic as possible, and therefore it does not support TCP/IP communication. It uses User Datagram Protocol (UDP) over IP on the one hand, and more efficient protocol than HTTP or REpresentational State Transfer (REST) API, or similar on the other hand. It uses fewer resources than HTTP and implements more features than HTTP such as observe, execute and discover features, also, to read and write. A performance comparison between HTTP and CoAP is inspected for energy consumption and response time in [10]. Observe means that the server or another device will observe whether there is a change in the state and notify about the change only. Discover feature included in CoAP to find devices that are in the surrounding environment. Moreover, a typical IoT platform could propose a variety of 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 of communication between devices. So, it is not a machine to machine communication. It consists of three elements, subscriber, publisher and broker. Then the clients are 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. Regarding security, MQTT supports Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

CoAP versus MQTT

There is always question what the best IoT protocol is? The answer depends on which type of application of IoT is used. In WAN network case, MQTT is better due to the concept of the broker. The broker is the middle of communication between devices. It will be useful in limited bandwidth such as different remote 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 an excellent 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 few UDP messages are to be sent, the CoAP will be better to be used instead of the Transmission Control Protocol (TCP) based MQTT.

IV. WHY DO WE USE THE IOT PLATFORMS?

IoT is a common type of technology; it has an aggregation of devices, sensors, software, and networks that work simultaneously to release the reliable and useful data from the Internet of Things. All these components are to be implemented together into an IoT platform.

IoT is not limited to include the communication ability of the things. It is an aggregation of devices, sensors, software and networks, that work together to release the beneficial and

useful data from the Internet of Things. Recently, an IoT platform could coordinate various essential aspects that lead to achieving IoT goals. This contains how to define a specific endpoint joint to a network, where and how the data is collected, at the end to find the best way for using the gathered information to lead the business significance. Therefore, the primary purposes of using IoT platforms are as follows.

First, IoT networks and multi-network connectivity. Recently, various types options of network technology were used to link IoT devices. However, the best choice of the networking solution depends on how and where it will be installed, as long as the required standard of service is guaranteed. Therefore, an inclusive IoT platform should support the communication and provide with all essential IoT types to display the most significant flexibility for recent and future projects.

Second, IoT service management, using an IoT platform is an important point to get better managing of the work and business and also to improve the capacity, and optimize operations. To keep on IoT solutions continually working, essential to managing the data and IoT networking simultaneously. IoT platforms should provide administration for accessing the user-controlled software tools to retain managing the endpoints 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 platforms could be managed efficiently for enhancing the IoT deployments[8].

Third, IoT data management and application enablement, for orchestrating data. Most of IoT solutions impact various sensors that can produce a high volume of data over time, such as condition, location, and status. Data streams composed and stored from the collected information. Each data point is usually short, while the amount of information received rapidly, relying on the reporting frequency of IoT devices. An IoT platform supports the ability to secure and normalize the data from different IoT endpoints, practically any sensor and any device reading. Multiple methods are sending streams of information and after receiving information could perform fragmentation, so the collected data can be processed efficiently, used, or reacted depending on the data obtained through applying the commands.

Fourth, analytics, statistic processing and data management by various data connections and hardware have to provide a useful result with accurate data analytics. The farthest aim of collecting the data is to fuel better business outcomes through increased visibility and insight. An IoT platform could support complete information and view of data analytics and capabilities that can extract the data and retain business from shipwright of new information that might organize weakly. IoT platform will have analysis performed, as well as the capability to rise specific third-party analytics software via secure API and services.

Finally, Security with multiple layers is one of the leading aspects to be considered for any business in IoT. Centralized and distributed low-level protocols including privacy and security for IoT as described in the survey [9]. Following necessary protection, rules to reduce the dangerous and increase the benefits of leveraging new sets of connected devices.

V. What is the role of an IoT platform?

IoT platforms play an 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 visualization of data at end application services.

IoT platforms provide connectivity service as a component of IoT platform and there are unique connectivity platforms that connect the customers and their devices such as SIGFOX which a provider of low-power and long-range connectivity, HOLOGRAM which is a cellular connectivity platform that provides inexpensive SIMs and CISCO JASPER which was acquired by Cisco in 2016 as a cellular connectivity management platform [10]. Security in IoT platforms means providing a secure connection to 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, [11] 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 challenging question for a company is how to select the suitable IoT platform to from a massive 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 in a particular IoT platform [12].

- The stability of the platform: Throughout plenty of platforms on the market, it has some likelihood that some will fail. It is essential to choose a platform that has high availability, i.e., the probability of being operational with no outage to be around several years, furthermore, the investment might be wasted if the platform provider fails. 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 will work not only for few endpoints in the beginning but also with growing needs during the time. Along with the scalability, the platform

should be flexible to keep up with speedily varying protocols, technologies, or features. It is also crucial that the platform has to be network agnostic. This means that it can integrate and work with all vital tech systems out there, rather than be locked into one vendor.

- The pricing model and the business case: A platform provider should be consequent in pricing. Some providers offer a prefatory rate and after that rise it up significantly when the contract has been retained. Also, the assigned budget for a platform to be selected is mostly the most effective factor of the consideration. There are some platforms that provide introductory prices and after selecting and subscribing to it, many features which are not needed or which are required are found. Also, platforms that are a concern on saving time have more costly operations, but platforms that will save money might not contain the whole competitive features. For instance, some of IoT platform vendors provide IoT platform with the ability to save money, but the announced platform does not contain all features which are provided by a vendor. In general, the company which offers more features will survive longer.

VII. Review of today's IoT platforms

Recent studies turn attention to the fact that there are more than 30 IoT platforms [13][14][15] used by different companies, and this number is further overgrowing. Moreover, the listed platforms in the schedule are not the same. Mobility management companies, innovative startups, hardware, security and network equipment are all in competition to become the best and lead IoT platform in the market. It is obvious from the table below, that few IoT platforms fully support device control management capabilities.

Moreover, there is comparatively few support for analyses of the produced IoT information regarding both visualization and computation. Majority of IoT platforms listed real-time support analytics that is a must be in any IoT framework. On the other hand, visual interface of data via graphical frontends mostly focused on simple patterns of the web portal. Those panels provide authorization to manage IoT ecosystem. However, few support the ability of visual data analytics[16].

In this section, we present 20 different IoT platforms according to their appropriateness into the particular application domains. It is evident that there are too many more platforms present in the market, but due to tech-specific and time limits 20 of these are chosen to provide accurate ideas about how they work, what are their strengths, what are their weaknesses, in which domain they are appropriate. While, studying and comparing these IoT platforms, each of these was tested in reality to distribute their advantages and disadvantages. Furthermore, based on applicability and appropriateness preferences in several domains the IoT platforms have been revisited. 20 different areas are selected and arranged alphabetically, depending on which most of IoT platforms are currently evolving into the IT market. While comparing the platforms chosen following parameters such as integration, security, a protocol for data collection, types of analytics support for visualization.

Platforms with Open-sources properties are considered to be more promising when comparing to the proprietary replacement for the following reasons. Firstly, using open source is predicted to become a faster combination of new integrated IoT solutions towards the scope of the application. Secondly, using IoT open source platforms has been declared to speed up the adoption process of a software technology in the bottom-up method [17] [14].

However, just a few platforms do not have a REST API. This observation predicts that an existing IoT services will tend to become closer to general web services (i.e., Web of Things [15]). Indeed, IoT service combines and will be merging the future key of IoT technologies [16][17][18]. We indicate that a few of platforms have connected some service discovery techniques even of a straightforward type. A general survey on M2M communication protocols can describe 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 architectures and their features, and the recent research addressing different aspects of the IoT. We must emphasize that in contrast to critical IoT applications we focused on mass IoT applications. Therefore the IoT platforms we surveyed mostly reflected the massive IoT requirements.

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 are framing the IoT. The description of our novel architecture represented in Section II might be useful.

Future works could present a detailed comparison and description of cloud 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

ACKNOWLEDGMENT

"This work was performed 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] 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] 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].

[8] 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.

[9] 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.

[10] 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].

[11] 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.

[12] 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].

[13] 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.

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

[15] 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.

[16] V. Gazis *et al.*, "A survey of technologies for the internet of things," in *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2015, pp. 1090–1095.

[17] J. Mineraud, O. Mazhelis, X. Su, and S. Tarkoma, "A gap analysis of Internet-of-Things platforms," *Comput. Commun.*, vol. 89–90, pp. 5–16, 2016.

[18] 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.

[19] 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.

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

[21] 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.