# Cloud for IoT - A Survey of Technologies and Security features of Public Cloud IoT solutions

Daniel Bastos
*BT Adastral Park Research Labs*
*British Telecommunications plc*
Ipswich, UK
daniel.bastos@bt.com

***Abstract*—All digital data that is produced nowadays is moving into the Cloud. Public Cloud providers offer unbeatable availability and redundancy of data in their servers, but the move to the Cloud is increasingly related to the associated services that it can provide. Internet of things devices are being deployed continuously with particular computing and storage constraints. This makes them perfect candidates for always being connected to the Cloud. Given the increasing importance of collected data, assuring end-to-end security between IoT devices and the Cloud is of paramount importance, with secure device authentication and encrypted communications as must-have features.**

**This paper provides a comprehensive study of public Cloud IoT solutions in the Platform-as-a-Service (PaaS) market. The focus is mainly on the security features, given that security is a weak spot in many IoT implementations. A comparison table was produced and the results show that popular standards are being used across providers for secure authentication and communications, while authorization is managed using diverse methods.**

***Index Terms*—Internet of Things, IoT, Security, Cloud, Platform, PaaS.**

## I. Introduction

The Internet of Things is finally starting to reach its true potential, with large scale deployments of more than 50,000 connected devices more than doubling in the last 2 years [1].

Deployments are in progress in all areas of business such as smart cities [2], industrial automation, healthcare [3], transportation, agriculture, retail [4] and also smart homes [5]. The opportunities for driving down costs and for productivity growth are making the case for IoT adoption. Data captured by sensors offers new categories of insight into business and people. When combined, streams of data can provide new forms of understanding on topics ranging from Economics to Biology.

However, harnessing the power of the data coming from IoT isn't straightforward. Sensors are meant to stay connected 24h a day/365 days a year, generating massive amounts of data. Hence, storing and analysing sensor data is a Big Data challenge. Studies reveal that most organizations do not have the analytics capabilities to take advantage of the data generated from IoT sources [6]. That's where the Cloud comes in, providing the infrastructure and the services to empower IoT deployments.

Security is an area of concern in IoT, in [7] the authors performed a comprehensive survey on IoT security in Smart Home and City environments, describing multiple security risks ranging from insecure credentials to attacks on communication protocols. As for Cloud computing, in [8] the authors performed an general analysis of security problems in Cloud computing, highlighting some issues and proposing a number of possible solutions.

This paper is organized as follows. Section II introduces the background on Cloud Computing, the different Cloud service types and the connection points between the Cloud and the IoT. Section III explains the methodology used in the analysis of the cloud solutions. Section IV presents the analysis of each cloud solution. In section V the findings discussed and in section VI conclusions are drawn on the work achieved.

## II. Background

According to the official NIST definition [9], Cloud Computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". The Cloud is historically associated with scalability. Pioneer Cloud providers saw an opportunity with the rising speeds of Broadband connections, investing a lot in computing and storage resources in order to rent them as a service. Small and medium enterprises (SMEs) were the main target because of their limited resources to buy such infrastructures, looking instead to rent them. As their need for computing power and/or storage increased or decreased over time, Cloud providers were able to scale the resources needed for each client, charging only for what they needed. The process of maintaining the infrastructure was also being taken care of by Cloud providers, resulting in a lot of savings for the SMEs.

With data being increasingly important, Cloud providers saw the opportunity to take advantage of the data they were storing in their infrastructure. Combining Machine Learning (ML) and Artificial Intelligence (AI) algorithms with powerful visualization tools allowed providers to start offering services around data analytics and business inteligence to their clients.

Moving into a world of all things connected, Cloud providers now offer dedicated IoT services. It's the culmination of two worlds coming together: small devices with low computing and storage that were used for simple offline

tasks (e.g. home garage system), and the always-on worldwide available Internet connected farm of servers.

### A. Cloud Service Types

The Cloud market is categorized into different types such as: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

Figure 1 details the differences between each model. Infrastructure as a Service (IaaS) is the most flexible cloud computing model, providing clients great control over the infrastructure. Here the clients have complete control of Applications, Data, Runtime, Middleware and Operating Systems and the Cloud provider only provides a dashboard or API to their Servers. This is the most popular option for SMEs.

Platform as a Service (PaaS) builds on top of IaaS and gives clients an environment in which most of the infrastructure is already taken care of, including Runtime, Middleware and Operating System. This allows clients to focus on developing applications and taking care of data. This is the most popular service type for IoT deployments, since clients just want to build a tailored application to run on each IoT device in order for it to connect to the Cloud to send and receive data.

Finally Software as a Service (SaaS) is the complete infrastructure as a service, including application and data. SaaS is the most familiar form of Cloud service for consumers in services like the Google Apps [10] or Microsoft Office 365 [11].

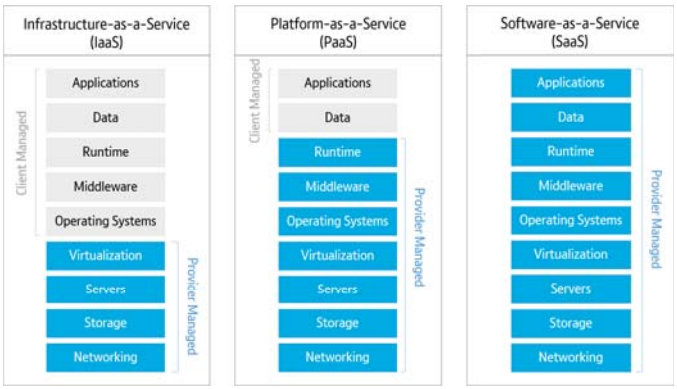


Fig. 1. Cloud Service Models

### B. What the Cloud means for IoT

As Figure 2 shows, there are multiple reasons why the Cloud provides value in IoT scenarios, so much so that Cloud connections have become a vital part of IoT deployments. The main advantage for IoT devices to be connected to the Cloud is the always-on remote access to the data they collect (e.g. a temperature sensor) and the actions they can perform (e.g. turn on a light). Then there are other features, like allowing easy bootstrapping and management of devices and unlimited data storage. A centralized dashboard provides enhanced data visualization and analytics.

In regards to security, the Cloud allows continuous asssessment of security levels in IoT connections, identifying security risks (e.g. insecure authentication) and providing guidelines on how to mitigate them. For developers, there's the interesting feature of programming triggers for certain actions, using Cloud services like AWS Lambda [12]. For example let's imagine a trigger for movements sensed by a motion sensor. A movement event will set off the trigger which has programmed a set of actions, like sending an email to the owner of the sensor with the information about the movement and/or turning on the surrounding lights and an alarm sound. This can all be programmed through the AWS Lambda service and run continuously without any human intervention.

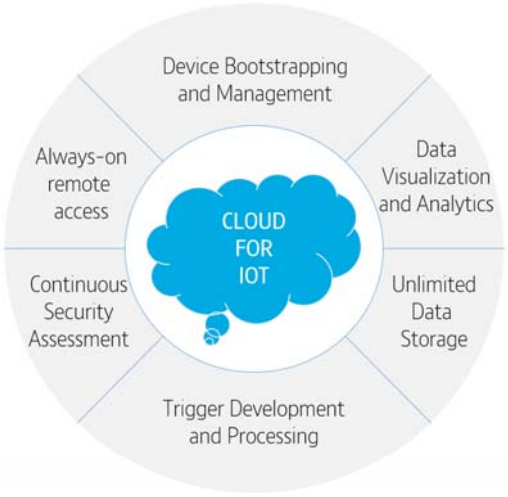


Fig. 2. Cloud for IoT

## III. Methodology

In this survey, the approach taken was to first select the most relevant Cloud providers in the IoT space, considering market share and services offered. The selected providers were: Amazon AWS [13], Microsoft Azure [14], Google Cloud [15], IBM Watson IoT [16] and ARM Mbed [17]. Their PaaS IoT product offerings were studied in detail in regards to supported technologies and protocols, with a special focus on security features.

### A. Hardware Support

The first feature to consider is hardware support. There are a number of popular IoT devices in the market that Cloud providers should support, such as: Raspberry Pi 2 and 3, Beagleboard, and other ARM Cortex-M or Cortex-A based devices. There are also Arduino devices (Uno, Yun) and Espressifs ESP8266 board which are very popular and not based on ARM processors.

### B. Associated Storage Services

PaaS solutions provide access to database and object storage services. These allow highly scalable and performant access to

data. For each Cloud provider their associated services were studied.

### C. Dedicated OSes and SDK Support

There are multiple dedicated Operating Systems for IoT devices, with the advantage that most are open-source. Examples of IoT dedicated OSes are: Raspbian [18], FreeRTOS [19], Riot [20], Contiki [21], Open-WRT [22], DD-WRT [23], Windows 10 IoT (Core and Enterprise) [24], Android Things [25] and Mbed OS [26].

Software Development Kits (SDKs) are provided by Cloud providers to allow developers to easily build applications that communicate with the Cloud IoT service. SDKs are built using different programming languages, the most popular in IoT implementations being: Embedded C, C, C++, C# (.NET), Java, Python and Node.js.

### D. Serverless Compute Services

As previously referred in II-B, there are Cloud services that allow the set up of triggers for certain conditions. Developers can upload code to be run in the Cloud as a response to each trigger. The service will automatically run the code when the trigger conditions are met, without requiring the user to provision or manage any servers. This is very useful in IoT environments because it can allow automation of multiple tasks without human intervention.

### E. Data protocols supported

IoT devices require lightweight protocols that allow quick transfer of data with low overhead. Examples of data protocols that are used in IoT scenarios are: Message Queue Telemetry Transport (MQTT) [27], Constrained Application Protocol (CoAP) [28], Advanced Messaging Queuing Protocol (AMQP) [29], Extensible Messaging and Presence Protocol (XMPP) [30], Quick UDP Internet Connections (QUIC or GQUIC) [31] and Data Distribution Service (DDS) [32]. The standard HTTP web protocol is also often used in IoT solutions. Some protocols like MQTT and AMQP support being used over Websockets [33].

### F. Security resources supported

Security resources are spread across diferrent properties: Authentication, Authorization, Encryption in transit, Encryption at rest and Availability. Let's assume availability related to the Cloud solutions themselves isn't and an issue considering it's their big selling point, so let's focus on the other properties. The Secure Sockets Layer or Transport Security Layer (SSL/TLS) protocol support is mandatory for any type of online communications, providing strong methods for authentication and encryption in transit. The most recent version is TLS 1.2. Datagram Transport Layer Security (DTLS) is the TLS protocol version for communications over UDP and also provides strong security features. X.509 Certificate support for authentication is part of TLS and DTLS and provides certificates (a public key and an identity) in order to authenticate users with the Cloud service and vice versa, as it can provide server authentication and device authentication. For client authentication the private key is stored on the IoT device for later use. Technologies such as the hardware Trusted Platform Module (TPM) [34] can be used for this step. Hardware root of trust implementations such as ARM's TrustZone [35] can also be used for strong authentication. OpenConnect ID (OIDC) [36] is an authentication layer protocol built on top of OAuth 2.0. OAuth 2.0 [37] is an authorization framework heavily used by online services. A dedicated authorization framework for IoT environments based on OAuth 2.0 is being actively developed by IETF [38]. This framework is called Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth). The combination of authentication and authorization techniques is often called Identity and Access Management (IAM) solutions.

## IV. Cloud IoT Services

The studied Cloud IoT services all aim to offer reliable and secure device-to-cloud and cloud-to-device connectivity, scaling to millions of devices and allowing easy device monitoring and management. For application development, SDKs are available for developers to build custom experiences to match business requirements. In addition, these services support the processing of billions of messages and allow enhanced data visualization. Finally, integration with other Cloud services provides an array of extra features like data analytics and serverless computation.

### A. AWS IoT Core

Amazon is the biggest player in the Cloud market. Their Amazon Web Services (AWS) platform offers a wide range of solutions for big and small businesses. The AWS IoT Platform was announced in 2015 [39] and was the first IoT dedicated Cloud service.

Their solution for IoT device connection and management is called IoT Core and integrates with a combination of other IoT services [40] like: AWS IoT Device Management, AWS IoT Device Defender, Amazon Greengrass, AWS IoT Analytics, AWS IoT Events, AWS Things Graph, AWS IoT SiteWise and AWS Lambda.

Each device connected to IoT Core is represented as a Device Shadow. A device shadow maintains an identity and last known state of a specific device and provides a channel to send and receive messages. When a message is posted to a device IoT Core will ensure the message is delivered even if the device is offline, because it will be delivered once the device reconnects.

Amazon has taken over the development of dedicated IoT Operating system FreeRTOS, providing tight integration with their services. In regards to language support, Amazon provides SDKs [41] in C++, Embedded C, Java, Python, JavaScript and dedicated ones for Arduino Yun, Android and iOS. MQTT is the only protocol supported for data communications, with the option of being over Websockets. A secure HTTP(S) REST API is available for communication with other services and apps. Authentication is possible using X.509

certificates, their own IAM tools, AWS Cognito and also Federated Identities. Authorization can be performed using Amazon's AWS IoT Policy and IAM roles. Encryption in transit is assured by TLS 1.2 and encryption at rest is available using the AES-256 algorithm. Amazon provides IoT Core with availability of over 99,9%, as defined in their Service Level Agreement (SLA).

### *B. Azure IoT Hub*

Azure is the Cloud platform of Microsoft. It has evolved rapidly over the last few years in order to keep up with AWS. On February 4 of 2016, Microsoft announced the general availability of their first dedicated IoT cloud solution, Azure IoT Hub Platform [42].

IoT Hub now integrates with a number of other Azure IoT services like [43]: Azure IoT Edge, Azure Stream Analytics, Azure Cosmos DB, Azure Functions and others.

Microsoft has its own dedicated IoT Operating system Windows 10 IoT (Core and Enterprise) which provides tight integration with their Cloud services and TPM chips on devices [44].

In regards to language support, Azure provides SDKs in C, C# (.NET), Java, Python and Node.js. MQTT, HTTPS and AMQP are the protocols supported for data communications, with the option of MQTT and AMQP being over Websockets. A secure HTTP(S) REST API is available for communication with other services and apps. Authentication is possible using X.509 certificates, OpenID Connect and SAS Tokens. Authorization can be performed using OAuth 2.0 and Azure's Active Directory Roles. Encryption in transit is assured by TLS 1.2 and encryption at rest is available using the AES-256 algorithm. Azure provides IoT Hub with availability of over 99,9%, as defined in their SLA.

### *C. Google Cloud IoT Core*

Google launched Cloud IoT Core Platform in February of 2018 [45]. Cloud IoT Core [46] integrates with a number of other Google Cloud services like: Cloud IoT Edge, Cloud Functions, Cloud Pub/Sub, Cloud Dataflow Cloud Machine Learning and others. Google has its own dedicated IoT Operating System Android Things which provides tight integration with their Cloud services.

In regards to language support, Cloud IoT Core provides SDKs [47] in C, Java, Python and Node.js. MQTT is the only supported protocol for data communications. A secure HTTP(S) REST API is available for communication with other services and apps. Authentication is possible using X.509 certificates and JSON Web Tokens. Authorization can be performed using OAuth 2.0 and Google's IAM Roles. Encryption in transit is assured by TLS 1.2 and encryption at rest is available using AES-128 and AES-256 algorithms. Google provides Cloud IoT Core with availability of over 99,9%, as defined in their SLA.

### *D. IBM Watson IoT*

IBM launched IBM Watson IoT Platform in December of 2015 [48]. Watson IoT [49] provides SDKs in C, C#, Mbed C++, Embedded C, Java, Python, Node.js and Node-Red. MQTT is the only supported protocol for data communications and can be used over Websockets. A secure HTTP(S) REST API is available for communication with other services and apps. Authentication is possible using X.509 certificates, OpenID Connect, IBM Cloud App ID. Authorization can be performed using IBM's Cloud IAM Roles. Encryption in transit is assured by TLS 1.2 and encryption at rest is available using multiple algorithms. IBM provides Watson IoT with availability of over 99,5%, as defined in their SLA.

### *E. ARM Mbed Pelion*

ARM launched Mbed Pelion in October of 2018 [50]. Pelion is advertised as a PaaS but also offers the option of being deployed On Premises, which means clients can run the entire service on their own private infrastructure. ARM has developed its own dedicated IoT Operating System called Mbed OS which provides tight integration with their Cloud services and TrustZone chips on ARM processors. Pelion [51] provides SDKs in C# (.NET), Java, Python, JavaScript and TypeScript. CoAP is the only supported protocol for data communications and OMA LwM2M for device management. A secure HTTP(S) REST API is available for communication with other services and apps. Authentication is possible using X.509 certificates. Encryption in transit is assured by TLS 1.2 and ARM has its own TLS library called MbedTLS [52] which allows lightweight implementations of the TLS protocol for low computing power devices. Encryption at rest and availability information isn't publicly available as far as was possible to assess. In April of 2018, ARM and IBM announced a software bridge solution connecting Arms Mbed Pelion with the IBM Watson IoT platform [53] which benefits both providers and their clients.

## V. Discussion

The analysis performed reveals that Amazon's IoT Core, Microsoft's Azure IoT Hub, Google's Cloud IoT Core and IBM's Watson IoT provide feature-packed solutions for IoT deployments. ARM's Mbed Pelion is very recent so it's still at an early stage, although it has strong points like Mbed OS, Mbed TLS and TrustZone root of trust integration with their processors.

During the study some things became clear: the amount of documentation available is both impressive and sometimes insufficient. AWS and Azure came on top on this item, providing the clearest and most detailed documentation. Another relevant aspect was related to maturity. AWS, Azure and IBM have an extensive portfolio of successful case studies related to IoT deployments, leaving Google and ARM behind.

Dedicated OSes and serverless compute services proved to be useful to offer a more complete end-to-end solution, Watson IoT lacking the dedicated OS component and Pelion lacking a serverless compute service.

In regards to security, all solutions showed support for TLS 1.2 and X.509 certificates, with AWS IoT Core and Azure IoT Hub being the most versatile when it comes to

TABLE I
FEATURES OF CLOUD IOT SOLUTIONS

| **Solutions / Features** | ***Amazon AWS IoT Core*** | ***Microsoft Azure IoT Hub*** | ***Google Cloud IoT Core*** | ***IBM Watson IoT*** | ***ARM Mbed Pelion IoT*** |
|---|---|---|---|---|---|
| **Cloud Service Type** | PaaS | PaaS | PaaS | PaaS | On Premises, PaaS |
| **Hardware Support** | All devices | All devices, >1000 certified IoT hardware devices | All devices | All devices | ARM Cortex-M and Cortex-A MCU based devices |
| **Associated Storage Services** | Amazon DynamoDB, Amazon S3 | Azure CosmosDB, Azure Blob | Google Cloud Bigtable, Google Cloud Storage | IBM Cloudant, IBM Cloud Object Storage | None |
| **Dedicated OS** | Amazon FreeRTOS | Windows IoT | Android Things, Android | None | Mbed OS |
| **Language/SDK Support** | C++, Embedded C, Java, Python, JavaScript, Arduino Yun, Android, iOS | C, C#, Java, Python, Node.js | C, Java, Python, Node.js, iOS | C, C#, Mbed C++, Embedded C, Java, Python, Node.js, Node-RED | C# (.NET), Java, Python, JavaScript/Typescript |
| **Serverless Compute Services** | Amazon Lambda | Azure Functions | Google Cloud Functions | IBM Cloud Functions | None |
| **Data Protocols** | MQTT, MQTT over Websockets, HTTPS, HTTP(S) REST API (JSON) | MQTT, MQTT over WS, AMQP, AMQP over WS, HTTPS, HTTP(S) REST API (JSON) | MQTT, HTTP(S) REST API (JSON) | MQTT, MQTT over WS, HTTP(S) REST API (JSON) | CoAP, OMA LwM2M, HTTP(S) REST API (JSON) |
| **Authentication** | X.509 Certificates, AWS IAM, AWS Cognito, Federated Identities | X.509 Certificates, OpenID Connect, SAS Tokens | X.509 Certificates, JSON Web Tokens (JWT) | X.509 Certificates, OpenID Connect, IBM Cloud App ID (Beta) | X.509 Certificates |
| **Authorization** | AWS IoT Policy, AWS IAM Roles | OAuth 2.0, Azure Active Directory Roles | OAuth 2.0, Google IAM Roles | IBM Cloud IAM Roles (Beta) | Mbed Cloud Policy (ACE-OAuth) (Beta) |
| **Encryption in Transit** | TLS 1.2 | TLS 1.2 | TLS 1.2 | TLS 1.2 | TLS 1.2 (MbedTLS), DTLS |
| **Encryption at Rest** | AES-256 | AES-256 | AES256, AES128 | AES-256, AES-128, RC4-128 | No info |
| **Availability (SLA)** | ≥99.9% | ≥99.9% | ≥99.9% | ≥99.5% | No info |

support for authentication methods. Encryption at rest is a standard feature in all Cloud providers except ARM Mbed Pelion which didn't provide information about this item. One interesting detail is that MQTT and HTTP are the most supported data protocols, being the only ones supported by some solutions. This choice is questionable from a security perspective, given that MQTT and HTTP only have cleartext username/password authentication and don't provide any data encryption or integrity features. For MQTT, the advantages of being a lightweight protocol are reduced because of the fact that it needs to be secured with the TLS protocol. Other lightweight protocols, such as AMQP and QUIC, offer more security features by default.

Table I presents a comparison of the features of each Cloud IoT solution studied.

## VI. CONCLUSION

This paper has analysed the core IoT Platforms offered by a number of relevant public Cloud providers, providing a comprehensive picture of the Cloud IoT space. Cloud IoT solutions were studied with respect to security features, supported technologies and protocols. A table was compiled presenting the different supported features for each provider. The analysis verifies that providers are taking security seriously and supporting popular standards. Still, some providers appear more advanced with regards to provided security features, offering superior solutions for IoT Cloud deployments.

## ACKNOWLEDGMENT

I acknowledge financial support for this work provided by the European Commission's Horizon 2020 research and innovation programme under the grant agreement No. 675320 (NeCS).

## REFERENCES


[1] IoT Barometer 2017/2018: number of large scale IoT projects doubled in one year. Available: https://www.i-scoop.eu/internet-of-things-guide/large-iot-projects-2017-2018-analysis/, acessed in January 2019.

[2] CityVerve. Available: https://cityverve.org.uk/, acessed in January 2019.

[3] Kit-Check Case Study. Available: https://aws.amazon.com/solutions/case-studies/kit-check/, acessed in January 2019.

[4] Advantech Case Study. Available: https://customers.microsoft.com/en-gb/story/advantech, acessed in January 2019.

[5] iRobot Ready to Unlock the Next Generation of Smart Homes Using the AWS Cloud. Available: https://aws.amazon.com/solutions/case-studies/irobot/, acessed in January 2019.

[6] Unlocking the business value of IoT in operations, Capgemini Report. Available: https://www.capgemini.com/wp-content/uploads/2018/03/dti-research_iot_web.pdf, acessed in January 2019.

[7] D. Bastos, M. Shackleton and F. El-Moussa, "Internet of Things: A survey of technologies and security risks in smart home and city environments," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 2018, pp. 1-7. doi: 10.1049/cp.2018.0030

[8] Almorsy, M., Grundy, J. and Mller, I., 2016. An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

[9] Cloud Computing definition, NIST. Available: https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published, acessed in January 2019.

[10] Google Apps. Available: https://get.google.com/apptips/apps/, acessed in January 2019.

[11] Office 365. Available: https://www.office.com/, acessed in January 2019.

[12] Amazon AWS Lambda Available: https://aws.amazon.com/lambda/, acessed in January 2019.

[13] Amazon AWS. Available: https://aws.amazon.com/, acessed in January 2019.

[14] Microsoft Azure. Available: https://azure.microsoft.com/, acessed in January 2019.

[15] Google Cloud. Available: https://cloud.google.com/, acessed in January 2019.

[16] IBM Cloud. Available: https://www.ibm.com/cloud/, acessed in January 2019.

[17] Mbed Cloud. Available: https://cloud.mbed.com/product-overview, acessed in January 2019.

[18] Raspbian OS. Available: https://raspbian.org/, acessed in January 2019.

[19] FreeRTOS. Available: https://freertos.org/, acessed in January 2019.

[20] RIOT-OS. Available: https://www.riot-os.org/, acessed in January 2019.

[21] Contiki OS. Available: http://www.contiki-os.org/, acessed in January 2019.

[22] Open-WRT. Available: https://openwrt.org/, acessed in January 2019.

[23] DD-WRT. Available: https://dd-wrt.com/, acessed in January 2019.

[24] Windows 10 IoT. Available: https://developer.microsoft.com/en-us/windows/iot, acessed in January 2019.

[25] Android Things. Available: https://androidthings.withgoogle.com/, acessed in January 2019.

[26] Mbed OS. Available: https://www.mbed.com/en/platform/mbed-os/, acessed in January 2019.

[27] MQTT. Available: https://mqtt.org/, acessed in January 2019.

[28] CoAP. Available: http://coap.technology/, acessed in January 2019.

[29] AMQP. Available: http://www.amqp.org/, acessed in January 2019.

[30] XMPP. Available: https://xmpp.org/, acessed in January 2019.

[31] QUIC. Available: https://www.chromium.org/quic, acessed in January 2019.

[32] DDS. Available: https://www.omgwiki.org/dds/, acessed in January 2019.

[33] What are Websockets. Available: https://pusher.com/websockets, acessed in January 2019.

[34] Trusted Platform Module. Available: https://trustedcomputinggroup.org/res ource/trusted-platform-module-tpm-summary/, acessed in January 2019.

[35] ARM TrustZone. Available: https://www.arm.com/why-arm/technologies/trustzone-for-cortex-m, acessed in January 2019.

[36] OpenID Connect. Available: https://openid.net/connect/, acessed in January 2019.

[37] OAuth. Available: https://oauth.net/, acessed in January 2019.

[38] L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman and H. Tschofenig, "Authentication and Authorization for Constrained Environments (ACE)", draft-ietf-OAuth-ACE-authz-10 (work in progress), February, 2019.

[39] Amazon Announces AWS IoT, Amazon Blog. Available: https://aws.amazon.com/blogs/aws/aws-iot-now-generally-available/, acessed in January 2019.

[40] Amazon AWS IoT Solutions. Available: https://aws.amazon.com/iot/, acessed in January 2019.

[41] Amazon AWS IoT Developer Guide. Available: https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html, acessed in January 2019.

[42] Azure announces Azure IoT Hub, Microsoft. Available: https://azure.microsoft.com/en-us/blog/azure-iot-hub-ga-capability-overview/, acessed in January 2019.

[43] Azure IoT Cloud Services. Available: https://azure.microsoft.com/en-us/services/#iot, acessed in January 2019.

[44] Windows 10 IoT TPM Support. Available: https://docs.microsoft.com/en-us/windows/iot-core/secure-your-device/tpm, acessed in January 2019.

[45] Google announces Cloud IoT Core, Google. Available: https://cloud.google.com/blog/products/gcp/the-thing-is-cloud-iot-core-is-now-generally-available, acessed in January 2019.

[46] Google Cloud IoT Core. Available: https://cloud.google.com/iot-core/, acessed in January 2019.

[47] Google Cloud IoT Core Documentation. Available:https://cloud.google.com/iot/docs/, acessed in January 2019.

[48] IBM Announces Watson IoT. Available: http://www.iotleague.com/ibm-announces-watson-iot-to-bring-power-of-cognitive-computing-to-a-connected-world/, acessed in January 2019.

[49] IBM Watson IoT. Available: https://internetofthings.ibmcloud.com/, acessed in January 2019.

[50] ARM announces Pelion. Available: https://blog.mbed.com/post/release-pelion-oct-2018, acessed in January 2019.

[51] Pelion Documentation. Available: https://cloud.mbed.com/docs/current/welcome/index.html, acessed in January 2019.

[52] MbedTLS Library. Available: https://tls.mbed.org/, acessed in January 2019.

[53] ARM and IBM simplify IoT and data analytics. Available: https://developer.ibm.com/iotplatform/2018/04/23/arm-ibm-simplify-iot-data-analytics/, acessed in January 2019.