A Secure Hybrid Cloud Enabled Architecture for Internet of Things

Avani Sharma*,Tarun Goyal†, Emmanuel S. Pilli*, Arka P. Mazumdar*, M. C. Govil*, R.C. Joshi‡
*Department of Computer Science and Engineering, Malaviya National Institute of Technology, Jaipur, India
†Department of Computer Science, Government Engineering College, Bikaner, India
‡Chancellor, Graphic Era University, Dehradun, India
Email: {avnisharma2010, tarungoyal.it, chancellor.geu}@gmail.com, {espilli.cse, apmazumdar.cse, mcgovil.cse}@mnit.ac.in

***Abstract*—Rapid advances in digitalization, Internet and world wide web enable the communication between two computing hosts across any location in the globe. Pervasive or ubiquitous computing enhanced this to a level that any two intelligent physical objects can communicate with each other, anytime and anywhere. Internet of Things (IoT) is a novel paradigm emerging from ubiquitous computing that facilitates communication between many real world objects by collaboration of various technologies. Integrating IoT with Cloud Computing derives manifold advantages to store and process enormous data generated by heterogeneous devices. Though both the technologies together have profound effect in many application areas like smart home, smart agriculture, healthcare etc., their integration involves many challenges. Security is one of the most important issues confronted by IoT-Cloud architecture. In this paper, we propose a Secure, Hybrid, Cloud Enabled architecture for IoT (SHCEI), which uses hybrid cloud (both public and private cloud). This architecture ensures security of intradomain data and will also address issues of scalability and interoperability. Further, we highlight some of the research challenges in implementing the combined architecture of Cloud and IoT.**

***Keywords*-IoT; Hybrid Cloud; Social IoT; Security; Scalability; Interoperability;**

I. Introduction

We have entered the third generation of World Wide Web i.e. Web 3.0 with the proliferation of Ubiquitous and Pervasive Computing [1]. The new era of Web 3.0 emphases on connecting real objects and people to the internet by ensuring ubiquitous communication between them. Internet of things (IoT) is one of the emerging technologies governed by Web 3.0 that brings new revolution in the field of ubiquitous communication. IoT was introduced in 1999 by Kevin Ashton of Massachusetts Institute of Technology (MIT) at Auto-ID Center with the concept of integrating radio frequency identification (RFID) and sensors [2]. IoT provides machine-to-machine communication (M2M) between smart objects with distributed intelligence and decision making capacity through integration of several technologies like sensors, actuators, identification, tracking, and enhanced communication protocols [3][4]. Characteristics of IoT devices are low power consumption, light weight, battery operated, limited computational, and storage capacity. Resource constraints in IoT devices restrict efficient deployment of IoT in various emerging fields like medical, transport, logistics where large amount of data is collected, and needs high computational power. Efficient IoT deployment in these fields require sufficient resources to provide larger storage capacity for heterogeneous, high density data generated by different source.

Cloud computing [5] is one of the supporting architectures that facilitates the resource and computational requirement of IoT architecture. Driving force behind using cloud computing as a reference is its configurable resources and its services that can be provisioned as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [5][6]. Though many advantages can be derived with cloud enabled IoT, integrating cloud in wireless, mobile, resource constraint IoT environment involves many challenges like massive scaling, identification of objects, object naming, heterogeneous networks, mobility support, architecture dependency, security & privacy, protocol mapping, robustness etc. [7]. Security is one of crucial issues that needs to be addressed to provide an efficient and reliable communication of data in IoT environment.

Heterogeneous network of IoT devices imposed with various security risk of distinct homogeneous netwoks forming it. In literature, various architectures have been proposed that implement IoT with cloud but none of them consider intra-level security of information and services. For establishing a secure communication environment, users should be provided with certain access rights with in a particular domain. A hybrid cloud structure can be used to facilitate this functionality. This paper presents a Secure, Hybrid, Cloud Enabled architecture for IoT i.e. SHCEI that uses both private and public cloud to ensure security and access with in a particular domain. We propose Adaptation Layer in SHCEI that uses private cloud for intra-networking of information to facilitate security. It also addresses issues of scalability and interoperability in heterogeneous IoT environment. Adaptation Layer also grabs the advantages of federated cloud by sending/receiving data, resources and functionalities between different private clouds via internet.

Rest of our paper is organized as follows. Section II gives

978-1-5090-0366-2/15/$31.00 ©2015 IEEE

a glance on existing solutions for IoT-cloud architectures with the need of designing new architecture. Section III explores various issues involved in integrating cloud with IoT. Section IV presents our proposed architecture SHCEI in detail followed by its application area. Section V discuss some applications that can be derive using SHCEI architecture. In Section VI, challenges with proposed architecture have been discuss. Finally, Section VII concludes our paper with a discussion on possible future research directions.

II. Existing Solutions

IoT and Cloud are distinct technologies that are evaluated independently. Integration of Cloud with IoT is required to provide sensing devices with the facility of data storage and solution for energy related issues [8]. In this section, we will discuss several existing architectures with their working scope and limitations.

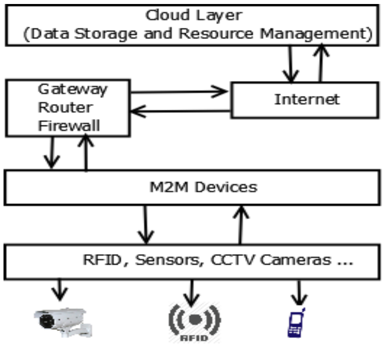
Cloud Layer
(Data Storage and Resource Management)
Gateway
Router
Firewall
Internet
M2M Devices
RFID, Sensors, CCTV Cameras ...
RFID

Figure 1. Basic Architecture for IoT-Cloud Integration.

IoTCloud [9] is a platform that controls and manages the sensors and messages over the cloud online with the different modules like Controller, Message Broker, Sensors, Client and GPS sensor. Controller is responsible for managing the components of system. Message Broker handles the low level details of message routing. Sensors are used by smart object to sense the clients, objects, targets and their availability. Client subscribes to sensor data to utilize specific application. GPS sensor module establishes connection between sensors, M2M devices and IoTCloud controller. This architecture uses FutureGrid Cloud services instead of GAE, Amazone EC2, and Microsoft Azure platforms [10].

CloudThing [11] provides infrastructure for developing, deploying, operating, and composing applications and services online. It provides the service platform, developer suite and operating portal, which works over the IaaS, PaaS and SaaS services of cloud. It uses Constrained Application Protocol (CoAP) to provide a request/response interaction model between application end-points. It works over the IPv6-based Low Power Wireless Area Network (6LoWPAN) for defining message frame format, fragmentation methods, and header compression techniques, which is required to fit IPv6/UDP datagrams in the very limited IEEE 802.15.4 frame size.

OpenIoT [12] architecture is a SaaS based open source architecture. In this architecture sensors communicate directly with the M2M devices and cloud contains databases only. Sensors have to communicate with the Cloud through web portal for any data.

Architectures discussed above can be implemented in the field of research, health, management, awareness, security, and etc. Sensors can connect to M2M devices directly and then M2M devices communicate with the cloud server using protocols such as CoAP, SOAP and RESTful Web Services. All the discussed architectures use only public cloud (GAE, Microsoft Azure, Amazone EC2, FutureGrid etc.) which increases security risk. There is no concept of hybrid cloud for managing things on the private and public together. These architectures implement all the resources and functionalities on their own in the starting phase of deployment. In case of any new resource requirement, user has to change and deploy the whole system again. Also, there is no concept of resource sharing between the clouds available. Problems present in the existing architectures are addressed upto certain extent in our proposed architecture SHCEI.

III. Integration Issues in IoT and Cloud

Despite of offering manifold advantages, integrating Cloud with IoT involves various issues [7] as depicted in Figure 2.

A. Communication

- Flow of data from enormous IoT objects to cloud for storage, computation and maintenance creates latency in responding of desired output. This delay can be caused by unnecessary processing at IoT device in multihop communication.
- Highly dense data from heterogeneous IoT devices have both necessary and unnecessary data. Transfer of unnecessary data may not be required all the time. This flooding of data results in inefficient resource utilization at cloud side of IoT.

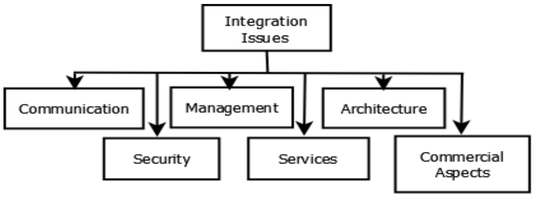

Figure 2. Issues Involved in integrating Cloud with IoT.

B. Security and Privacy

- One of the major issues that needs to be addressed while communicating in cloud-IoT environment is security. Wireless nature of IoT makes them vulnerable towards different kind of insider and outsider security attacks. An intruder can interrupt the ongoing communication either between the IoT devices or between the IoT network and cloud interface. Infected communication between IoT and cloud adversely affects the reliable and efficient data storage on cloud.

- With new types of devices and heterogeneous networks, users employ wide range of public methods to access the digital world. It is impossible for an individual to control the adapted global method that capture personal information of user. Also with the availability of larger storage, personal information of user maintained for longer period that allows disclosure of their personal information. Use of cloud to facilitate data storage of IoT creates privacy problem by allowing global access to information to all the users.

C. Management

- Resource scheduling in cloud environment are required to dynamically prioritize the requests and to serve them in real time. It is a very difficult task for cloud manager to decide how much a particular resource may be required by a device.
- Managing huge amount of data that consist of high-valued information mixed with dirty and erroneous data is a challenging task.
- Tracking mobile objects to manage their identity and location is an issue in cloud-IoT environment. Clouds have to update the information about objects corresponding to their location to provide ubiquitous and seamless communication among objects.

D. Services

- Discovering new services for the users is responsibility of cloud manager (broker) in cloud enabled IoT. Characteristics of IoT, like joining or leaving the network by node at any moment, create challenges for cloud manager to discover new services.
- Objects in IoT differ with each other in many aspects, like processing power, bandwidth requirement, coverage and network interface (IP and Non-IP). Interoperability solution should be maintained to provide seamless interaction among objects to get accurate service description, publishing and discovery mechanism.

E. Architecture

- Protocol structure at device level that support cloud interface is required for proper realization of IoT with cloud. Existing protocols do not work well for low power, energy constrained IoT network. To support IoT with cloud, a standard architecture based on cloud computing at centre is required.
- Huge number of IoT devices can be identifying using IPv6. An efficient mechanism to support IPv4-IPv6 coexistence is required in Cloud-IoT architecture.
- Maintaining distributed objects on a single platform (i.e. on cloud) is an issue to be solved. With heterogeneous and distributed devices, clouds need to implement an interoperability mechanism that can provide interface for different devices to make network scalable.

F. Commercial Aspects

- From business point of view, integrating cloud with IoT involves issues of pricing services. The billing for resources utilized from the cloud depends on the services of cloud chosen. Though use of private cloud reduces security issues, cost of communication may increase. To deal with such cost-security trade off, an integrated approach should be use that combines public cloud with private cloud.

IV. Proposed Architecture: SHCEI

In this section, we propose SHCEI, an hybrid architecture to deploy IoT with cloud while keeping security as a vital requirement. The architecture of SHCEI, as shown in Figure 3, is segmented into four layers- Device Layer, Adaptation Layer, Internet Layer and Service Layer. In the following subsections we discuss each of these layers in brief.

A. Device Layer

The Device Layer forms the basis of SHCEI architecture where various smart objects, conforming to IEEE802.15.4 and IETF specifications for IoT, communicate with each other to share information. Different technologies can be adopted to enable communication between nodes (i.e. smart objects) based on the application requirements like:

- Wireless Sensor Networks (WSN) for low power, low cost sensor motes.
- Mobile networks for seamless connectivity.
- Ethernet for reliable, connection oriented communication.

WSN [14] together with Radio Frequency Identification (RFID) [15] is most adapted technology to enable communication between physical objects. RFID system consists of multiple RFID tags (attached to objects to provide unique identity) and few RFID readers (to read identity of objects). RFID tag can use either 64 or 96 bit code to store unique ID of objects based on the EPCglobal standard. Wireless sensor nodes, equipped with various sensors acquire data in different forms (text, signal, image, and video) in real time and communicate among themselves either directly or using multihop communication. These objects form clusters of different domains according to the applications. Each cluster has one or more coordinating nodes, designated as the master nodes, that control the working and communication between other nodes. Master nodes have more power and energy compared to the other nodes, or the slave nodes. The slave nodes communicate either via master node or in ad hoc fashion. All the master nodes in a cluster forward

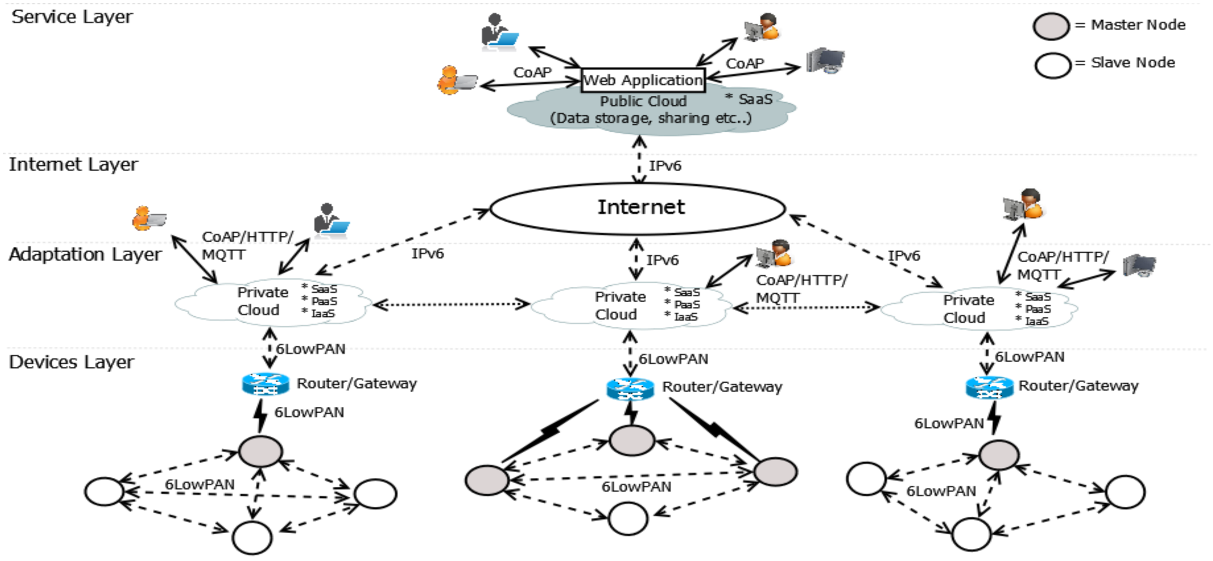

Figure 3. Framework of Proposed Architecture: SHCEI

data to the adaption layer through a specific gateway, which provides the possibility of forming heterogeneous networks. Various microcontroller, presently available in market, that can be used to build IoT with different sensors, are Arduino, Raspberry pi, Beagle Bone Black etc [16].

In mobile communication, the devices communicate with each other using mobile networks provided by various carriers throughout the world. Hence, these devices can move freely between the coverage areas seamlessly and communicate through mobile gateways.

Ethernet, though it is mainly used for communication from gateway to the upper layers, can also be used for some sensing devices in scenarios where the node need not move from places and where reliable communication is needed. For example, some master nodes may need secure and reliable connection to the gateway and use ethernet instead of wireless medium.

B. Adaptation Layer

Having public cloud for data access and services, security of information may be compromised by the outsiders. Private clouds have certain policies described by specific organization for data access to restrict the users from getting all type of services. To ensure security of data within a single domain, data gathered from the Device Layer is first stored to a private cloud through gateways. This layer provides data storage in private cloud within an organization where clouds offer services like SaaS, Paas and IaaS to its intra-domain users.

Web services over cloud use RESTful [17] and SOAP architecture [18] to offer light weight services. REST adopts CRUD (Create, Read, Update, and Delete) operations provided by the HTTP protocol such as GET, POST, PUT, and DELETE. SOAP manages the sensor's data and their geographical working location. User can use web application through HTTP [19], CoAP [20] or MQTT [21] protocols. Constraint Application Protocol (i.e. CoAP) is a RESTful application layer web transfer protocol used between low power embedded wireless networks using HTTP interfaces. CoAP incurs less parsing complexity, low overhead, and runs on top of User Datagram Protocol (UDP). Hyper-text Transfer Protocol (i.e. HTTP) is a simple text based protocol that supports many libraries. HTTP client in IoT devices (small devices of 8-bit micro controller) works in half duplex mode and highly complex TCP. Message Queuing Telemetry Transport Protocol (i.e. MQTT) is specially designed to support lossy networks with small overheads of nearly 2 byte per message. It is used to publish and subscribe data transport with efficient bandwidth but it doesnt provide device-to-device transfer or multicast.

The integration of WSN and the web using REST/CoAP with web applications (REST/HTTP) through CoAP/HTTP proxy, helps to visualize the measurements of WSN on the HTTP web browser based on CoAP. Security of the data is maintained by the Datagram Transport Layer Security (DTLS) protocol. Use of private cloud at each domain restricts information access to the outside users, which in turn ensures the security of data within a specific domain.

In SHCEI architecture, users can also share data, resources, and functionalities with other private cloud by using internet on the conceptual, logical, and procedural level and this technology is known as Cloud Federation. One organization can extend their working area in future to one more geographical location with new technologies and protocols. To share data and resources between different locations, there is no need to upgrade old setup. Adaptation Layer not only ensures security using private cloud but also consider the issues of scalability and interoperability in heterogeneous IoT environment. Having distinct private cloud to process heterogeneous data collected from different IoT devices reduces complications involved in operating heterogeneous data on the same cloud. Bringing enormous data on the same platform and accessing it using standard protocols solves interoperability issues. Though, introducing adaptation layer in Cloud-IoT environment derives significant advantages, issue of extra data overhead might be present in SHCEI. We will discuss it with the other research challenges in Section VI.

C. Internet Layer

Internet Layer provides global communication for information exchange between different private clouds. Data from these private clouds can then be processed and uploaded to a public cloud, so that it can be accessed globally by the users. This layer also communicate resources, and functionalities between private-private or private-public clouds using Internet. The concept of Cloud Federation, discussed in the previous subsection, can also be realized in this layer as it provides the means of communication between clouds. To facilitate large number of devices in IoT, all the protocols and hardware used in this layer must support IPv6 for internetworking.

D. Service Layer

Users access services or data across different organizations through a public cloud. The public cloud provides SaaS and access to shared data globally. CoAP/HTTP/MQTT protocols, integrated with RESTful and SOAP architecture, can be used to access various web services which helps visualize the data acquired by WSN.

V. Applications of SHCEI

SHCEI can be useful in various domains where secure data communication is needed, like healthcare and Social-IoT (SIoT). In healthcare, automation has become a prime factor to process and store the information about patients, doctors and other staff. Diagnosis of patients require knowledge about their condition and various medical records by the respective doctor. Many of these information are confidential and not disclosable. The adaptation layer of SHCEI provides this possibility.

Another area where SHCEI can be implemented is SIoT which integrates concept of social networking with IoT. SIoT needs secure communication of information to enable social networking between different organization/institute or domain. In Social IoT, the things autonomously establish social relationships among themselves with respect to the the persons attached to them to provide improved communication and collaboration among human and things. However, intelligence of the things will be limited to a local optima if it includes a single manufacturers domain. The problem can be resolved by leveraging information from multiple and collaborative social networks. Along with the advantages gained through this collaboration, one major issue that will also propagate is privacy of information. Sharing of information among these social networks should consider the sensitivity of user and ensure protection of privacy of people. Similar to the previous example, the privacy requirement in this case can also be managed by the adaptation layer of SHCEI.

VI. Research Challenges

Though our proposed architecture SHCEI provides a novel framework to deploy IoT with cloud, some integration issues are involved with SHCEI architecture that need to be addressed. Some of the important issues are discussed here:

1) Overheads: Use of private-public cloud system in SHCEI architecture gives rise to the overheads. Data communication between private-public clouds and between private-private clouds generate unnecessary overheads that in turn affect the computational time, memory, bandwidth and other resources of cloud.
2) Data Transmission: Transmission of data in Cloud-IoT environment requires an effective identity management of IoT devices to deliver underlying quality of services. Identification of huge number of IoT objects can be done using IPv6 addressing. SHCEI architecture needs to implement an efficient mechanism for IPv4-IPv6 coexistence.
3) Data Integrity: Use of private-public cloud structure creates data integrity problem in SHCEI architecture. Apart from that, data transferred between different clouds generate redundant information. An efficient mechanism to handle redundant data and to maintain data integrity is required in proposed architecture to ensure effective and reliable service delivery to the users.
4) Resource Management: To effectively and efficiently utilize the cloud services, management and scheduling of resources are important. It is difficult to determine when and how much resources are required. There is a need to implement an efficient resource management algorithm and scheduling mechanism at both private and public clouds of proposed framework.
5) Protocol Mapping: Although SHCEI architecture uses standard protocol structure that conforms to IEEE and IETF specification, mapping of protocol for different type of devices and at different level of cloud is an important issue. In order to maintain interoperability between IoT devices, an effective mapping mechanism is required in proposed architecture.
6) Federated Cloud: Sharing resources and technologies between different clouds of different networks in SH-

CEI architecture involves various challenges. Private Clouds are imposed with certain policies and laws by the organization, under which the cloud is used. To use services of other cloud, some protocols should be followed which permit access to cloud services. An architecture that uses list of available resources at each cloud and signing SLA between clouds on the basis of logical and conceptual level is required.

7) Pricing: One of the most important aspect of any architecture is its cost of implementation. Deployment of SHCEI suffers pricing issue because of implementing both private and public clouds for data storage. Use of private clouds at each intra domain incurs high cost that may not be feasible in a cost constraint application environment.

VII. Conclusion

We have proposed SHCEI, a secure hybrid private-public cloud architecture which provides security to the heterogeneous network data in IoT environment, while ensuring scalability and interoperability. We have discussed various integration issues while bringing these two all-encompassing technologies to talk to each other and derive mutual benefit from respective strengths and provision great services to users. We have added an adaptation layer in proposed architecture which implements private cloud to provide secure and seamless communication between the network and sensors. We have made use of Cloud Federation to address the issue of security and communication between distinct private clouds. Some of the research challenges encountered with proposed architecture are also discussed.

In future, we would like to address the research challenges and develop a prototype model of IoT-Cloud which will secure data of both inter and intra level networks. We will try to implement proposed architecture for real time scenario to ensure its applicability. We envision that our future approach would be cost effective, highly secure, using minimum resources, built on most efficient protocols and have proper service level agreements in place for data and resource sharing.

References

[1] J. Hendler, “Web 3.0 Emerging,” Computer, vol. 42, no. 1, pp. 111-113, 2009.

[2] http://postscapes.com/internet-of-things-history.

[3] J. Tan and S. G. M. Koo, “A Survey of Technologies in Internet of Things,” in IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), 2014, pp. 269-274.

[4] L. Atzori, A. Iera, and G. Morabito,“The internet of things: A survey,” Computer Networks, vol. 54, no. 15, pp. 2787-2805, June 2010.

[5] P. Mell and T. Grance, “The NIST definition of cloud computing,” 2011.

[6] B. B. P. Rao, P. Saluia, N. Sharma, A. Mittal, and S. V. Sharma, “Cloud computing for Internet of Things & sensing based applications,” in 6th International Conference on Sensing Technology (ICST), 2012, pp. 374-380.

[7] M. Aazam, I. Khan, A. A. Alsaffar, and E.-N. Huh, “Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved,” in 11th International Bhurban Conference on Applied Sciences and Technology (IBCAST), 2014, pp. 414-419.

[8] A. Botta, W. de Donato, V. Persico, and A. Pescape, “On the Integration of Cloud Computing and Internet of Things,” in International Conference on Future Internet of Things and Cloud (FiCloud), 2014, pp. 23-30.

[9] https://sites.google.com/site/opensourceiotcloud/.

[10] G. C. Fox, S. Kamburugamuve, and R. D. Hartman, “Architecture and measured characteristics of a cloud based internet of things,” in International Conference on Collaboration Technologies and Systems (CTS), 2012, pp. 6-12.

[11] J. Zhou, T. Leppanen, E. Harjula, M. Ylianttila, T. Ojala, C. Yu, H. Jin, and L. T. Yang, “Cloudthings: A common architecture for integrating the internet of things with cloud computing,” in 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD), IEEE, 2013, pp. 651-657.

[12] J. Mineraud, O. Mazhelis, X. Su, and S. Tarkoma, “Contemporary Internet of Things platforms,” arXiv preprint arXiv:1501.07438, 2015.

[13] N. Mitton, S. Papavassiliou, A. Puliafito, and K. S. Trivedi, “Combining Cloud and sensors in a smart city environment,” EURASIP Journal on Wireless Communications and Networking, vol. 2012, no. 1, pp. 1-10, 2012.

[14] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” Computer networks, vol. 38, no. 4, pp. 393-422, 2002.

[15] S. Hodges and D. McFarlane, “Radio frequency identification: technology, applications and impact,” Auto-ID Labs White Paper Series, vol. 1, 2005.

[16] http://postscapes.com/internet-of-things-hardware.

[17] A. Rodriguez, “Restful web services: The basics,” IBM developerWorks, 2008.

[18] G. Alonso and F. Casati, “Web services and service-oriented architectures,” in 21st International Conference on Data Engineering, ICDE, p. 1147.

[19] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, “Hypertext transfer protocol–HTTP/1.1,” 2070-1721, 1999.

[20] Z. Shelby, K. Hartke, and C. Bormann, “The constrained application protocol (CoAP),” 2014.

[21] U. Hunkeler, H. L. Truong, and A. Stanford-Clark, “MQTT-S–A publish/subscribe protocol for Wireless Sensor Networks,” in 3rd International conference on communication systems software and middleware and workshops, comsware, 2008, pp. 791-798.