# Software Defined Networking Managed Hybrid IoT as a Service

Peter Edge
Department of Computing
Ara Institute of Canterbury
Christchurch, New Zealand
email: peter.edge@ara.ac.nz

Zara Davar (Zahra)
Department of Teaching, Learning and Design
Ara Institute of Canterbury
Christchurch, New Zealand
email: zara.davar@ara.ac.nz

Zhongwei Zhang
School of Computational and Environmental Sciences
University of Southern Queensland
Queensland, Australia
email:zhongwei.zhang@usq.edu.au

***Abstract*— In the new era, communication devices use the Internet and World Wide Web to communicate from different locations around the world. The Internet of Things (IoT) extends this communication paradigm within different smart devices by collaborating sensor technology. In this model, infrastructure components must manage the large amounts of data generated by the smart devices and sensors. Integration of cloud computing with the IoT has many benefits and challenges; for example, cloud computing can improve the management of data from the collection phase to data process and backup. The most prominent challenges resulting from the integration are privacy and security. In this paper, we propose a secure hybrid cloud architecture mix with edge and fog computing to address security and privacy issues of IoT data. Our approach is to distinguish public and private data in the device data collection layer and address them to the right cloud (public or private) taking advantage of Software Defined Networking (SDN) for design and management of the networking layer. The privacy and security issues will be addressed within the design of the networking layer, in which all the necessary rules and protocols are in place and implemented.**

***Keywords-Internet of Things; Hybrid Cloud; Security; Privacy and Software Defined Networking.***

## I. INTRODUCTION

The new era of digitalization and communication aims to connect smart devices and real objects via the Internet. The landscape of Internet-based communications has been dramatically changed by the IoT [7]. IoT relies on intelligent devices interconnected within a dynamic global network infrastructure using the sensor technology to communicate with other smart devices [1] [8]. It is possible to use the IoT technology to create "robots" out of devices surrounding us, to collect data from the smart devices, and then to make intelligent decisions in our day-to-day life [2].

IoT mainly uses cloud computing for data collection and management. Even though cloud computing and IoT are two different technologies, they have a complementary relationship in collecting and processing a huge amount of data.

On the one hand, the cloud is predominately the platform utilised for Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [9]. Also, most known cloud types are public, private and the hybrid clouds. The hybrid cloud is a mixture of a public and a private cloud. On the other hand, cloud computing involves the on-demand delivery of computer power, database storage, applications and other compute resources.

IoT requires the flexibility of resource design in its architecture. The resource design must cover large scale storage for massive amounts of IoT data generated by devices [7], although IoT uses cloud computing architecture to solve many of the IoT computational and resource issues. However, integrating cloud and IoT technologies presents challenges, such as scalability, identification of different type of data, and the management of unnecessary data, heterogeneous networks, security and privacy.

This paper provides an overview of existing cloud solutions for IoT security challenges as well as our proposed solution. The remainder of the paper is organised as follows: Section II includes basic concepts; Section III discusses existing solutions; our proposed solution, the integration of the software definitions of networking and hybrid IoT is presented in Section IV; Section VII concludes the paper.

## II. BASIC CONCEPTS

In this section, we introduce the fundamentals of cloud computing and Software Defined Networks (SDN). Cloud computing refers to a network of remote servers hosted on the Internet [3]. It has been divided into two categories: public and private cloud.

In the infrastructure design for the private cloud, single tenant physical servers are often the best choice. In this paper, we call single tenant physical servers bare-metal servers. Bare-metal servers are dedicated servers assigned to each client without any resource sharing. One of the main benefits of using bare-metal servers, besides performance, is security. A bare-metal server physically isolates your data, applications and other resources [6]. Using bare-metal servers will help in achieving high performance and a secure environment.

On the other hand, the public cloud uses virtual servers. In this model, computing and storage are shared by different users. This will decrease security and privacy as well as performance. One of the main benefits of using a public cloud is having a cost-efficient cloud environment. Hybrid cloud is a term used in cloud computing and refers to a cloud architecture consisting of both the public and private clouds. SDN, simply defined, is the physical decoupling of control

 ISBN: 978-1-61208-711-5 

and data planes within traditional networking elements. While the control plane is responsible for routing path decisions, the data, or forwarding plane, forwards packets based on the logical knowledge of the control plane.

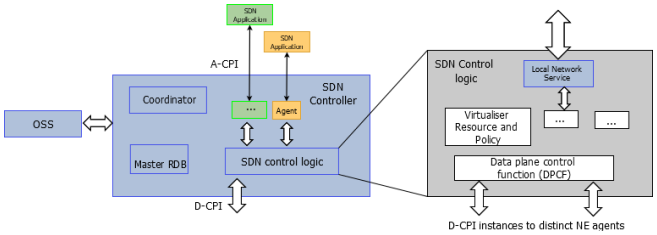


Figure 1. SDN controller logic

The result is a distributed model comprising a single controller influencing multiple forwarding devices. A representation of decoupling control and data planes is given in Figure 1. The biggest advantage for separating planes being the ability to control match criteria. Forwarding rules and flow match information can be injected via Application Programming Interfaces (APIs) available on the controller and distributed to forwarding devices via a secure link between controller and forwarder. OpenFlow is one such protocol utilised between controllers and switches.

Hybrid IoT as a service leverages the agility of what an OpenFlow-enabled network can offer. The ability to control flows is based on existing and extensible match fields. The programmability simplifies traffic engineering, providing an opportunity to craft custom match combinations and include priorities and action lists, or the ability to punt a matching packet to secondary match fields and actions.

## III. EXISTING SOLUTIONS

In this section, we present a critical review on the existing cloud computing solutions and discuss the gaps in the data challenges and security.

In an open source architecture called “OpenIoT”, web servers use sensors for data communication with the cloud [10]. In this solution, sensor communication with the cloud is through Representational State Transfer (REST) services and Simple Object Access Protocol (SOAP) protocol. This solution is based on the public cloud, which cannot cover security aspects for IoT data.

The Secure, Hybrid, Cloud Enabled Architecture for IoT (SHCEI) [11] solution presents a secure hybrid cloud design for IoT data security. In this architecture, the pure private cloud is placed in the device layer to collect IoT data. This solution provides a highly secure cloud solution for the IoT. However, using this approach generates an overload of unnecessary data. This will increase the number of cloud resources needed to manage the IoT data; this solution is not cost effective.

The idea of IoT data monitoring in an SDN-coordinated IoT-cloud has been introduced to ease the issue of data congestion in the IoT model [15]. In this research, using SDN flow steering makes available multiple paths for message delivery in IoT data usage, and performs monitoring of the data path in the network transport layer by using open source technologies. The problem with the design is how to distinguish and encrypt private IoT data before monitoring and delivering.

A solution proposed recently to address IoT data traffic is known as edge IoT analytics [16]. This research used SDN to manage data analytics at the edge cloud, stopping unnecessary data transfer to the next layer.

Meanwhile, another similar study proposed an IoT-aware SDN solution [17] to solve IoT data traffic congestion in the network edge. Even though these studies tackled the issue of IoT data traffic during transfer, synchronization between cloud components, SDN and IoT devices either had not been considered or is not an optimal and practical approach.

In another study, a Tenant Network (TN) has been proposed provide security in a multi-tenancy cloud environment for IoT data [18]. The idea of isolating all the network components to different zones such as the cloud controller, cloud administrator and tenant administrator was presented. This research improves trust between the cloud user and provider using TN architecture, although it cannot support distributed deployment with different controllers. Therefore, the approach cannot satisfy the IoT data scale.

In Edge Computing (EC), allocated applications, hosting happens at the edge servers [12]. EC is compatible with “private devices” such as smart phones, laptops, pagers, etc [13]. The aim of EC is to create a better quality of service for end users [13]. On the other hand, Fog Computing (FC) processes data at the LAN [14]. Therefore, fast and reliable data communication happens in FC. Both EC and FC will be used as part of our proposed architecture. Even though they are beneficial for IoT data collection and process, they need smart network architecture for the IoT data scalability issue. We will discuss this in Section V.

Although using cloud technology eases the management of IoT in many ways, there remain open gaps and challenges in this domain. Challenges such as data/resource management, communication, security, privacy and cost are the primary gaps in most existing cloud-IoT architectures. In this research we specifically address security and privacy issues in cloud based IoT architecture.

## IV. INTEGRATION OF SDN AND HYBRID IOT

The public and private clouds have their own set of rules for collecting, transferring, managing and processing data.

We propose to integrate the SDN with the hybrid cloud in the sensor layer of IoT data collection. The integration would fill the security gap between hybrid cloud computing and IoT from data collection to transfer and analysis using SDN at the device layer. It also allows us to tackle security challenges using integration of SDN and hybrid cloud architecture in an efficient way.

 ISBN: 978-1-61208-711-5 

Having an IoT hybrid cloud architecture mixed with SDN technology will address the security and privacy issues of IoT data (from collection to the analysis phase). This architecture will therefore be a significant improvement in IoT technology and will encourage enterprise clients moving towards IoT technology. The presented approach will minimise the chance of data leakage during data collection, transfer and analysis.

In this research, devices will be categorised as public and private devices. This categorisation can be varied for different cases; however, devices are considered private when the data generated by them is sensitive. For instance, personal communication devices, health-related devices, etc. Other devices are public devices such as entertainment devices, doors, windows, kitchen appliance. In our proposed SDN design, data collected from devices have to pass some security layers before they sit in the right platform. We address most of the hybrid cloud IoT issues using SDN at the device layer. We isolate and encrypt private data before its arrival in the private cloud.

## V. CASE STUDY

In this section, we will illustrate the integration and the proposed solution for security. The challenge is that different network rules apply to sensor devices from the IoT side and to those in the data collection in the hybrid cloud architecture.

In our proposed solution, Figure 2 represents the existing collection network for IoT data. Figure 3 represents an edge node configuration that integrates an SDN controller with an OpenFlow-enabled switch. For the test bed, as an initial experiment, we are collecting environmental data in the form of indoor temperature, humidity, CO2, and outdoor data from a weather station including wind speed, outdoor temperature, pollen and dust count. The edge node is also represented in Figure 2 as a point of demarcation for data arriving at the edge node.

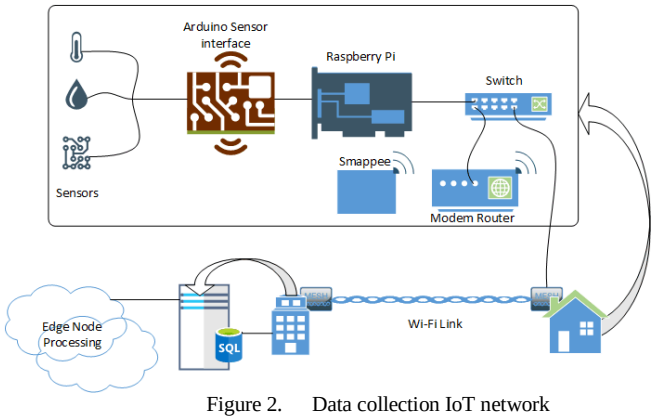


Figure 2. Data collection IoT network

Separating the collection of data represents a major area for this work. Collection examples from simple http header extraction locating embedded sensor serial numbers, to flow rules representing metadata and analog information from the devices to verify whether a transmission came from the expected transmitter in the expected location. In this way,

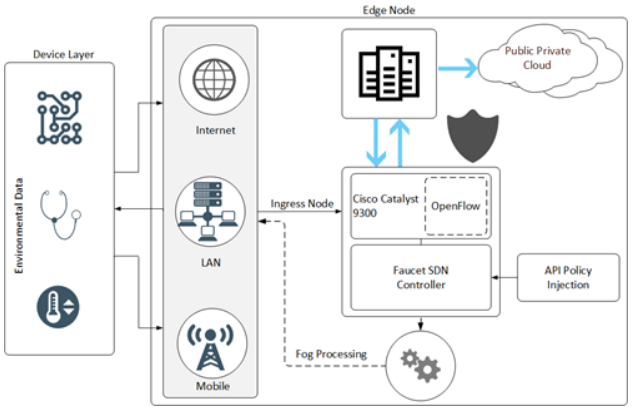


Figure 3. IoTaaS edge node design

proof of location and authentication from devices will provide a unique key. This combination of sensor data will provide the basis of flow tables to modify flows for the SDN controller.

Security between the buildings is handled by encrypting the point-to-point wireless link. All data arrives at the edge node having been collected from low power wireless (SigFox), 802.11, 4G or Ethernet.

Currently, site sensors represented in Figure 2, are hardwired through an Arduino, data is collected by a Raspberry Pi and sent point-to-point wirelessly between buildings. File transmission on the link is handled by Rsync. Encrypting at this point in the transmission network rather than at the sensor level takes a processing load off the sensor physical layer and ensures no additional burdens are placed on low powered sensors.

As data arrives at the Catalyst 9300 switch, OpenFlow match rules will segregate the data based on sensor location and the metadata generated by sensor hardware characteristics. Data will be sent to matching egress ports, depending on match and action rules. Some data will take the return path for correlation or further processing. In this phase, further processing will only be necessary for real time processes.

In the proposed solution, custom flow matches with the SDN controller, use the Openflow Extensible Match (OXM) and leverage the experimenter field.

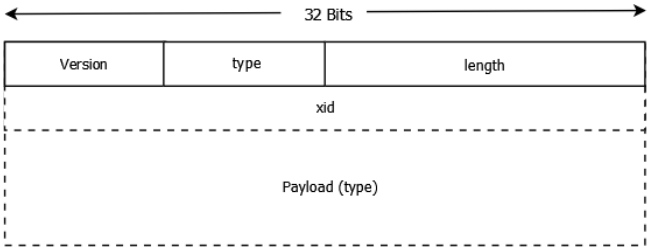


Figure 4. OpenFlow Header

Use of the experimenter field in OpenFlow requires the access to a vendor ID and is represented as class 0xfff which extends the header to 64 bits by using the first 32 bits of the

body as an experimenter field. Figure 4 shows the OpenFlow header. The experimenter field addition allows for matching of unknown and custom tables. For this work, matching criteria is based unique sensor metadata and characteristics.

As part of policy development, refinement and extending the range of rules based on flow matches within the OpenFlow controller, utilising external packet matching filtering will play a major role in the future of this project. The Berkeley Packet Filter (BPF) is one such set of filters able to optimise hardware ASICs [19].

Development of policy to optimise match rules already supported in OpenFlow V1.5 is focused on segregation of flows at the collection point for field networks Internet, LAN and Mobile. Match tables with corresponding flow instruction fields will separate data on interface, VLAN or both, as actions in response to flow matches.

Adding an experimenter OXM extension to the match fields of the SDN controller leverages the pipeline sequence processing employed by the OpenFlow protocol. Unique flows are identified by the combination of priority and match fields.

Flow entry instructions and action lists make it possible to pass packets to other flow tables or perform an action without further processing. This process could include re-writing packet headers in preparation for alternate egress ports based on flow type.

## VI. CONCLUSION AND FUTURE WORK

In this paper, the idea of integrating an SDN solution for managing Hybrid IoT data is presented. The aim is to use SDN to supervise efficient and secure Hybrid Cloud Computing to manage data collected by devices over the Internet. This design is leveraging the advantage of using Hybrid Cloud computing capability, storage and networking capability.

As a result, IoT will benefit from the performance, security and scalability of Hybrid Cloud Computing [1] while data collection and storage are managed by a secure network.

The emerging IoT paradigm challenges current network methods and practices. Network perimeters are potentially defined by the distribution of field devices deployed in homes, factories, agriculture and on-person. Beyond the issues of dealing with the flood of data generated from smart devices, addressing privacy and security is a priority for research. Private data traversing multiple network and storage domains pose perplexing issues for the integration of cloud computing and IoT.

Exponential growth of the IoT phenomenon has created a gap in the management of incoming-data processing. Furthermore, the inability to manage big data efficiently exacerbates the development of security processes for isolation of private sensitive data.

## ACKNOWLEDGMENT

We would like to thank Ara Institute of Canterbury for their support with providing the testing resources in the Cisco Networking Academy Lab during preparation for this paper.

## REFERENCES

[1] G. Fortino, A. Guerrieri, W. Russo and C. Savaglio, "Integration of agent-based and Cloud Computing for the smart objects-oriented IoT," Proceedings of the IEEE 18th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Hsinchu, pp. 1-6, 2014.

[2] A. Botta, W. de Donato, V. Persico and A. Pescapé, "On the Integration of Cloud Computing and Internet of Things," International Conference on Future Internet of Things and Cloud, Barcelona, pp. 23-30, 2014.

[3] Q. Erwa, L. Yoanna, Z. Chenghong and H. Lihua, "Cloud Computing and the Internet of Things: Technology Innovation in Automobile Service", Yamamoto, Sakae, Berlin, Heidelberg, pp. 173-180, 2013.

[4] B.B. P. Rao, S. Payal, N. Sharma, A. Mittal and S.V. Sharma. "Cloud computing for Internet of Things & sensing based applications". 2012 Proceedings of the International Conference on Sensing Technology, ICST. pp. 374-380, 10.1109/ICSensT, 2012.

[5] S. Muhammad and S.Tariq. "Cyber Security and Internet of Things", 2017 [Online: last accessed February 2019].

[6] https://www.rackspace.com/library/what-is-a-bare-metal-server. 2018, [Online: last accessed March 2019].

[7] A. Sharma, et al., "A Secure Hybrid Cloud Enabled architecture for Internet of Things," IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, pp. 274-279, 2015.

[8] A. Sharma, E. S. Pilli and A. P. Mazumdar, "Obviating capricious behavior in internet of things," 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, pp. 480-486, 2017.

[9] https://www.oracle.com/assets/2018-cloud-predictions, 2017, [Online: last accessed January 2019].

[10] J. Mineraud, O. Mazhelis, X. Su and S. Tarkoma, "A Gap Analysis of Internet of Things Platforms", Computer Communications, pp. 5-16, 2010.

[11] J. Mineraud, M. Oleksiy, S. Xiang and T. Sasu, "Contemporary Internet of Things Platforms", pp. 1-6, 2015.

[12] W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, "Edge Computing: Vision and Challenges," in IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646, 2016.

[13] E. Hesham, et al., "Edge of Things: The Big Picture on the Integration of Edge", IoT and the Cloud in a Distributed Computing Environment. IEEE Access. pp. 1-1, 2017.

[14] D. Puthal, S. Nepal, R. Ranjan and J. Chen, "Threats to Networking Cloud and Edge Datacenters in the Internet of Things," in IEEE Cloud Computing, vol. 3, no. 3, pp. 64-71, 2016.

[15] H. Yoon, S. Kim, Taekho Nam and J. Kim, "Dynamic flow steering for IoT monitoring data in SDN-coordinated IoT-Cloud services," International Conference on Information Networking (ICOIN), Da Nang, pp. 625-627, 2017.

[16] R. Vilalta, et al., "End-to-End SDN/NFV Orchestration of Video Analytics Using Edge and Cloud", OFC, 2017.

[17] R. Muñoz, et al., "IoT-aware Multi-layer Transport SDN and Cloud Architecture for Traffic Congestion Avoidance Through Dynamic Distribution of IoT Analytics", Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA), pp. 1-3, 2016.

[18] W. Dai, et al., "TNGuard: Securing IoT Oriented Tenant Networks based on SDN", IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1-13, 2018.

[19] S. Jouet, R. Cziva and D. P. Pezaros, "Arbitrary packet matching in OpenFlow," 2015 IEEE 16th International Conference on High Performance Switching and Routing (HPSR), Budapest, pp. 1-6, 2015.

 ISBN: 978-1-61208-711-5 