Realization of an Intrusion Detection use-case in ONAP with Acumos

Shabnam Sultana[*§], **Philippe Dooze**[†] and **Vijay Venkatesh Kumar**[‡]
[*]highstreet Technologies GmbH, Berlin, Germany
Email: shabnam.sultana@highstreet-technologies.com
[†]Orange Labs, Lannion, France
Email: philippe.dooze@orange.com
[‡]AT&T Services, Inc., New Jersey, USA
Email:vv770d@att.com
[§]Chair of Communication Networks
Technical University of Chemnitz, Germany
Email: shabnam.sultana@s2017.tu-chemnitz.de

***Abstract*—With Software-Defined Networking and Machine Learning/Artificial Intelligence (ML/AI) reaching new paradigms in their corresponding fields, both academia and industry have exhibited interests in discovering unique aspects of intelligent and autonomous communication networks. Transforming such intentions and interests to reality involves software development and deployment, which has its own story of significant evolution. There has been a notable shift in the strategies and approaches to software development. Today, the divergence of tools and technologies as per demand is so substantial that adapting a software application from one environment to another could involve tedious redesign and redevelopment. This implies enormous effort in migrating existing applications and research works to a modern industrial setup. Additionally, the struggles with sustainability maintenance of such applications could be painful. Concerning ML/AI, the capabilities to train, deploy, re-train, and re-deploy AI models as quickly as possible will be crucial for AI-driven network systems. An end-to-end workflow using unified open-source frameworks is the need of the hour to facilitate the integration of ML/AI models into the modern software-driven virtualized communication networks. Hence, in our paper, we demonstrate the journey of a sample SVM classifier from being a python script to be deployed as a micro-service using ONAP and Acumos. While illustrating various features of Acumos and ONAP, this paper intends to describe an end-to-end workflow by taking advantage of the integration of both the open-source platforms.**

***Index Terms*—ONAP, DCAE, Acumos, Microservice, Kubernetes, SDN, SVM, ML/AI, DDoS**

I. Introduction

With the advent of Software-Defined Networking(SDN) and the evolution of Machine Learning(ML), both academia and industry have demonstrated interests in utilizing them as the fundamental blocks for enabling an intelligent and automated communication network. While SDN has been accepted as a promising approach for future networks with features such as centralized control and network virtualization, machine learning is establishing its roots in communication networks through numerous research studies and practical applications [1]. However, in the prevailing era of technology evolution, even software development has witnessed tremendous developments and progression. This has led to such a substantial divergence of tools and technologies due to which adapting research studies and existing applications could involve significant effort in modification of its design and development. This could further create a substantial gap between research studies and industrial implementation in terms of performance and generic applicability when it comes to implementing and evaluating research outcomes in a real industrial or commercial network with real-time data. An unified open-source framework empowering possibilities of quick and easy migration of research or any existing application given any target environment is the need of the hour. With an aim to highlight such opportunities, we demonstrate a use-case of intrusion detection in an open-source platform named ONAP with the aid of another unified ML platform called Acumos.

Today's industries are migrating their standalone applications to scalable and resilient ones with more generalized configurations. One such strategy is the service-oriented microservice architecture which has earned popularity for implementing software in the form of fine-grained, distributed services with better portability, elasticity, robustness, and scalability [2]. In networking systems, Open Network Automation Platform (ONAP) is such a comprehensive platform for orchestration, management, and automation of network and edge computing services for network operators, cloud providers, and enterprises. Based on the microservice architecture, ONAP empowers product-independent capabilities for design, creation, and lifecycle management of network services, covering a broad spectrum of use cases for Communication Service Providers (CSP) [3]. ONAP addresses the rising need for a common automation platform for telecommunication, cable, and cloud service providers by offering vendor-agnostic, policy-driven service design, implementation, analytics, and lifecycle management for large-scale workloads and services orchestration for both virtual and physical network functions. On the other hand, Acumos is an open-source platform sup-

This work has been funded by the OptiCON project of Federal Ministry of Education and Research(BMBF), Germany.

porting onboarding, training, integration, and ML/AI deployment as containerized services (serving models). Thereby, Acumos endeavors to meet the demands of a broad range of business use cases by presenting a unified framework facilitating packaging, sharing, versioning, licensing, and deploying ML/AI models in the form of portable, containerized microservices, which are interoperable with one another [4].

In our demonstration, we present how an SVM (Support Vector Machine) classifier developed using Scikit learn and trained to detect DDoS (Distributed Denial of Service) attack traffic can be packaged by Acumos into a containerized model, then onboarded into the ONAP Data Collection, Analytics and Events (DCAE) platform, and then deployed as ONAP compatible microservice (DCAE service). The following sections are organized as follows: Section II gives an overview of related work with Acumos and ONAP and also few references of relevant academic work for DDoS Detection using SVM classifier. Section III provides a quick functional and architectural overview of the Acumos platform. Section IV offers a functional overview of ONAP components such as Data Collection, Analytics and Events (DCAE), Data movement as a platform (DMaap), and the Acumos Adapter. Section V provides the functional and technical illustration of our use-case and its demonstration. Section VI concludes our work with insights and the scope of future developments and demonstrations.

II. Related Work

In general, Acumos provides a platform to develop, onboard, and deploy ML and AI applications. Additionally, the Acumos marketplace offers a shared platform that helps to extend AI and ML applications to a wide range of industrial and commercial use-cases. It is to be noted that given a target environment, apart from deploying ML/AI models, re-tuning the model parameters post its performance evaluation is an essential and indispensable task. Tomorrow, the capabilities to train, deploy, re-train and re-deploy AI models as quickly as possible will be a crucial factor for AI-driven companies. By addressing these challenges of integrating ML models into application development, this generic open-source platform aims to meet the demands of a broad range of business use cases, including network analytics, customer care, field service and equipment repair, health care analytics, network security and advanced video services, to name just a few [4]. [5] presents the case study of packaging sentiment analysis and classification ML models via the Acumos platform, thereby demonstrating how the Acumos platform reduces the technical burden on application developers when applying machine learning models to their business applications. Furthermore, while addressing the use-case of ad effectiveness and how deep neural networks can be used for ad Click-Through Rate (CTR) optimization, [6] presents the benefits of using Acumos as the platform for implementation. Observing the four stages in the life-cycle of an Acumos solution, the authors describe how ad CTR predictions could be accomplished in a short span of time, thereby supporting businesses to shorten the decision-making process and reduce resource utilization.

While Acumos presents a new ML packaging and distribution platform [6], ONAP adds a new software component, namely "Acumos-DCAE Adapter" since its Frankfurt release, which provides a client interface to receive ML models from an Acumos catalog to ONAP DCAE. Only the integration of both these platforms was demonstrated using generic models into the DCAE-Model Onboarding and Design Tool (MOD). To the best of our knowledge, this work makes the first attempt to demonstrate an end-to-end flow of the framework beginning with the creation of a simple model to running it as an ONAP DCAE microservice.

There is a massive amount of research work for intrusion detection, including DDoS traffic detection using various ML/AI, including deep learning and transfer learning techniques. One of the ML methods that has been thoroughly studied in this regard is the SVM classifier. Based on an SDN environment simulated by mininet and floodlight, [7] refers to SVM as a good classification learning method without a lot of training data by demonstrating an average accuracy rate of 95.24 %. Similarly, [8] proposed a SVM-based model to detect the DDoS attacks on an experimental platform based on mininet and floodlight controller. They further analyzed other machine learning algorithms, such as decision tree, naive bayes, KNN, Random Forrest, to analyze the traffic and detect DDoS attacks, further proving that SVM can detect DDoS attack with higher accuracy and shorter time. Hence, we use the SVM classifier as the sample model in our demonstration. It is also to be observed that these experiments were mostly implemented as standalone applications on platforms simulated by standard network emulation tools like mininet. Therefore, the question arises not only on the scalability and robustness of these applications when deployed onto a commercial network, but also on the effort required to design and develop these models if they are to be deployed on a microservice-based networking system like ONAP.

III. A brief overview of Acumos

The goal of Acumos is to ease the daily life of data scientists by providing a secure environment to store, share and versioning their models and to enhance the deployment, and sustainability of AI models in industrial environments, thus scale up the introduction of AI-based software across a wide range of industrial and commercial problems. By providing an open-source mechanism for packaging, sharing, licensing, and deploying AI serving models in the form of portable, containerized microservices, it offers a unified framework for data scientists who can develop abstract AI models using various toolkits such as Scikit Learn, Tensorflow, H2O, C++ and ONNX, while enabling software developers to integrate the models into practical applications, without demanding to have knowledge or experience of the various AI toolkits employed by the data scientists [9]. The features of Acumos were very well exhibited by [6] using their case studies of sentiment analysis and image recognition with object detection.

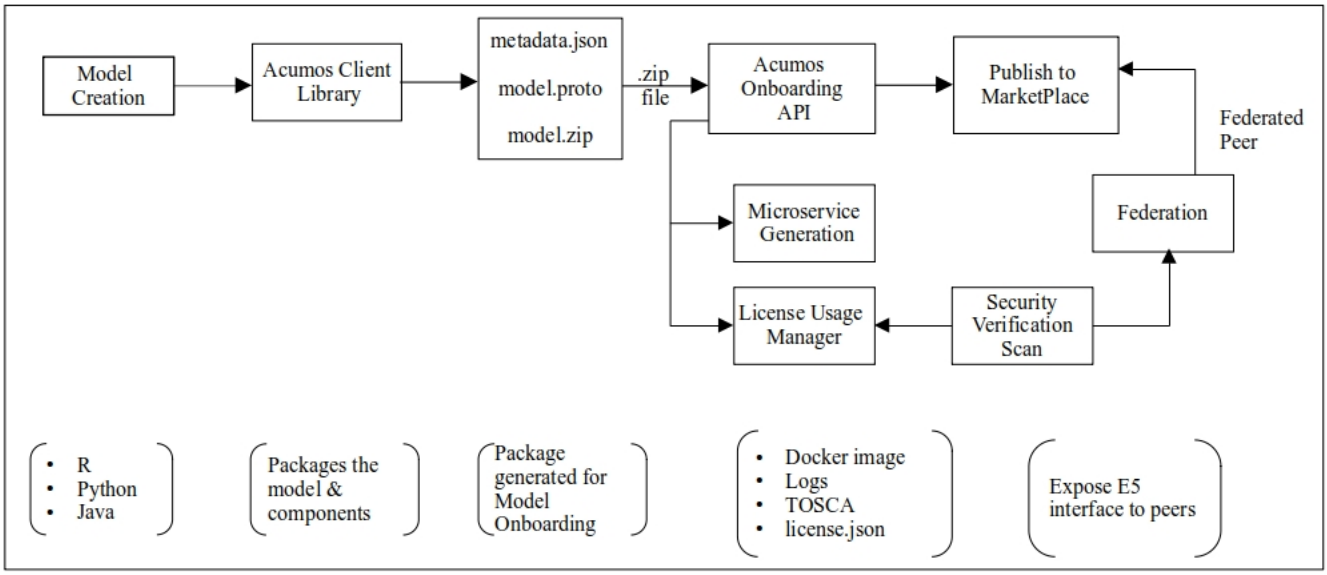

Fig. 1. Flow of packaging, onboarding and sharing of ML models using Acumos

Figure 1 gives a technical overview of different steps and components involved while Acumos supports the functionalities as mentioned earlier. As shown, Acumos supports various programming languages such as R, Python, Java, C++, and also models in ONNX format, allowing data scientists to create their models using appropriate tools such as Scikit learn, tensorflow. Acumos provides client libraries for each of these languages responsible for packaging the model for onboarding into the Acumos platform. The client library generates three files, namely metadeta.json with details of the model input and output, tools, libraries, and their versions used in the model development; model.proto, which is the protobuf definition of the model that is required to communicate with the microservice once it is deployed and running; and a model.zip file comprising of the user model and also an Acumos generated model needed by the onboarding API. These files packaged as a zip file are onboarded into Acumos using the onboarding API, providing a modeler to opt for microservice generation and license uploading. The microservice generation component generates the docker image from the model that could be downloaded or pulled and run in the corresponding environment. Lastly, the functionality of sharing and reusing of models is provided by the Acumos Marketplace, where modelers can publish the onboarded models into corresponding catalogs and allow sharing of models. The federation interface further enables the peers to access models from the shared catalogs of the Acumos Marketplace via the E5 interface.

IV. A BRIEF OVERVIEW OF ONAP-DCAE

ONAP provides a unified framework for vendor-agnostic instantiation and orchestration of physical and virtual network functions while meeting the challenges of scalability by developing global and massive scale (multi-site and multi-Virtual Infrastructure Manager (VIM)) automation capabilities for both physical and virtual network elements. From a functional point of view, ONAP comprises two main frameworks, namely "Design-time" and "Run-time" framework [10]. The design-time framework accommodates a comprehensive development environment with tools, techniques, and repositories for defining and describing resources, services, and products, including policies. The run-time environment executes the rules and policies distributed by the design and creation environment and the controllers that manage physical and virtual networks. Additionally, it is equipped with real-time monitoring capabilities through the Active & Available Inventory (A&AI) component that provides real-time views of a system's resources, services, products, and their relationships with each other [11]. The overall architecture of ONAP and the functionalities of its components have been very well summarized by [12] which proposes an active VNF placement strategy in the context of ONAP, which dynamically offloads request based on the load observed within a data center. In our work, we take a close look into its components, namely DCAE (Data Collection, Analytics, and Events) [13] and Data Movement as a Platform(DMaap) service. The DCAE platform is accountable for collecting, ingesting, transforming, and storing data as necessary for analysis, as well as providing a framework for the development of analytics. On the other hand, DMaap provides a secured and reliable data movement service between different components of ONAP acting as subscribers and publishers [14].

- DCAE (Data Collection, Analytics, and Events): As mentioned earlier, DCAE is the data collection and analysis subsystem of ONAP. The components of DCAE are classified into *Platform* and *Service* components. DCAE platform components are responsible for on-demand de-

ployment and management of the DCAE service components. Besides, the DCAE platform also configures the data paths between the service components, i.e., by setting up DMaaP topics and configurations. One notable platform component is the Cloudify Manager which can be termed as the lifecycle engine of DCAE and facilitates operations such as deployment, modification, allocation, configuration of various DCAE services, thereby facilitating activities such as multi cloud provisioning, monitoring, self-healing and scaling of compute resources [15]. DCAE service components are the virtual functional entities which realize tasks such as collecting measurement, fault, status, configuration, and other types of data from network entities and infrastructure that ONAP interacts with, as well as apply analytics on collected data. The Virtual Event Streaming (VES) collector, for example, is one such service component that supports the collection of individual or batch of events, while the Threshold Crossing Analytics (TCA) application offers an analysis of a performance metric based on a defined high and low threshold.

- DMaap (Data Movement as a Platform): This component is responsible for the movement of message data and data feeds between ONAP components using the pub-sub technology of Apache Kafka [14]. Apache Kafka is an event streaming platform that allows systems to publish (write) and subscribe(read) to event streams, along with storage and processing of these events. These events are real-time data from event sources like databases, network devices, cloud services, and software applications that are stored in "topics" [16]. Message Router is a RESTful web service provisioning end-points to clients (ONAP components) for publishing and subscribing to topics in Kafka. In our case study, we use this service of DMaap to subscribe to test data and publish prediction output.

Furthermore, since the Frankfurt release, DCAE provides the Acumos-DCAE adapter that can import ML/AI models from a specified Acumos instance by establishing a peer-to-peer connection with the Acumos platform and access its catalogs [17]. Nevertheless, it is to be noted that this adapter is still in the proof of concept stage due to the lack of an end-to-end use case.

V. Case Study

Regarding the environment setup, we have used the open standard cloud computing platform named Openstack [18] for provisioning the virtual servers on bare metal and Kubernetes [19] as the state of the art container orchestration system. We have the Clio release of Acumos installed on a single node Kubernetes cluster (not a minikube node) for our case study. The underlying VM consists of the recommended configurations as in the installation guide [20]. The ONAP framework has been installed on a Kubernetes cluster composed of 14 worker nodes and 3 controller nodes. Like Acumos, the standard installation process has been followed for ONAP using the ONAP Operations Manager(OOM) [21]. A brief overview of the resources and their corresponding configurations is provided in table I.

TABLE I
Resource requirements for Acumos and ONAP

Clusters	No. of VMs	Cores	RAM (in GB)	HDD(in GB)
Acumos	1	6	32	250
Full fledged ONAP Setup				
Controllers	3	4	8	80
Worker Nodes	14	8	16	80
NFS Server	1	4	8	320

In our paper, while considering the use case of intrusion detection, we demonstrate the journey of an SVM classifier from being a standalone python script to being deployed as a microservice in the ONAP platform capable of interacting with other components via the DMaap. We explain the end-to-end workflow describing the various features and components of Acumos and DCAE based on the demonstrations we made as part of our collaborations with ITU-T FG AN [22] and a leading network operator of Europe. A brief picture of the workflow is presented by Fig. 2.

We start with model creation, where we develop an SVM classifier to detect DDoS attacks with prediction output as '0' implying normal traffic and '1' indicating a DDoS traffic. The model is trained and tested on the NLS_KDD dataset [23]. We will refer to the model as *DDoSDetector* for the rest of our paper. Considering the DDoSDetector as a sample model for the demonstration of both platforms and their integration, the performance evaluation is out of scope in our demonstration. As the model is built using scikit learn in python, we use the python client library for packaging the model and generating its metadata and protobuf definition. A zip folder of the generated package as in Fig. 1 is then onboarded into the Acumos platform. With a successful onboarding along with microservice generation, we demonstrate how Acumos encapsulates any model while creating independent containerized microservices. The model is further published to a public catalog of the marketplace. We further configure the ONAP platform as a federation peer for Acumos, thereby allowing Acumos-DCAE adapter of ONAP to access the public catalogs and the models from the Acumos marketplace via the E5 interface. This phase of the case study exhibits how a data scientist can create ML/AI models serving specific use-cases without needing to create an end-to-end software application.

The second phase starts in the ONAP framework with the ONAP user using the Acumos-DCAE adapter to establish a peer-to-peer connection with the Acumos instance by supporting the E5 interface of Acumos. The primary functions of the Acumos-DCAE adapter are the following [17]:

- The adapter accommodates a DCAE model runner to transform the ML model from Acumos into a compatible microservice in the DMaaP environment. As DMaap facilitates the passage of data between ONAP components acting as publishers and subscribers (based on the pub/sub technology of Apache Kafka), the DCAE model runner

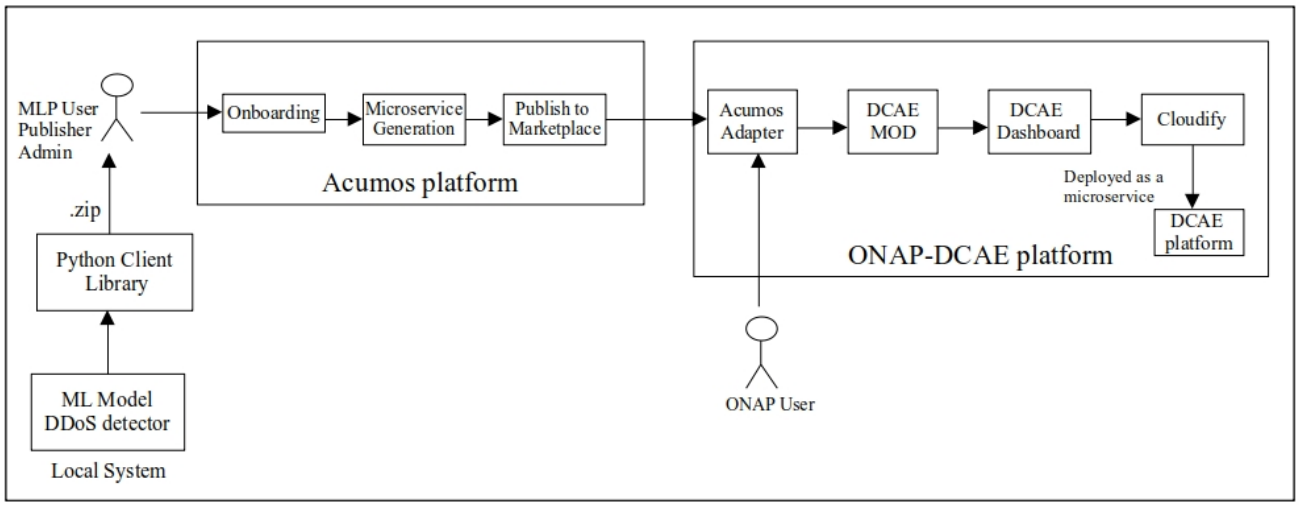

Fig. 2. End to end workflow of case study using Acumos-ONAP

maps each Acumos model method to a subscriber and a publisher stream. It further implements DCAE APIs such as health checks and configuration updates.

- The adapter generates automatically valid microservice metadata files (i.e., the componentspec.json and dataformat.json) for onboarding the model to the DCAE design environment.
- Lastly, the adapter generates the k8s/Docker executable image for onboarding to a secured registry provided during its installation.

Post importing our DDoS Detector from Acumos successfully, we use the DCAE Model and Onboarding Design (MOD) tool to create a processor from the imported Acumos Model. Comprising of components developed by the ONAP team and components taken from the Apache Nifi project, the DCAE MOD is responsible for onboarding, designing, and distributing microservices or a pipeline of microservices (DCAE Flows) to its distribution targets [24]. These targets are DCAE runtime environments that have been registered and are enabled to accept flow design changes that are to be orchestrated in that environment. In our case study, we do not create a process flow comprising of multiple DCAE components; instead, we generate and distribute the blueprints of the Acumos Model as a standalone service (no relationships with other DCAE components) to our registered target Kubernetes ONAP cluster. The blueprints are distributed to DCAE Inventory which can be viewed and updated through DCAE Dashboard. Worth noting that the DCAE platform provides a mechanism to provision secure topic/feed during deployment (by interaction with Dmaap Bus-Controller). The Cloudify Manager, as mentioned previously, is the lifecycle management engine of DCAE Services, hence takes the responsibility of deploying our DDoS Detector as a DCAE service that is capable of communicating with any other desired ONAP component using the DMaap message router. Thereby, as a result of our demonstration, we have our deployed microservice running in the ONAP platform as below in Fig. 3. As our model is deployed as a standalone service without connection to other DCAE components such as the VES collector, we use "curl" commands to publish test data samples into the message router topic *X_Test* using its REST API. The DDoSDetector could successfully subscribe to this topic, perform its ML prediction and publish the output for the corresponding test data into the topic *Classify_Out* which could also be accessed using curl commands.

VI. Conclusion

In this paper, we demonstrated an end-to-end deployment of a simple SVM classifier for DDoS detection as a microservice in the open source platform of ONAP aided by Acumos. By describing the involved steps and several components of Acumos and ONAP, we highlight the time and effort reduction that is accomplished for tasks such as the generation of a docker image or microservice or creating the required component specification and blueprint files for microservice deployment. Automation of such tedious tasks by Acumos and ONAP should allow data scientists and researchers to stay focused in their domain without taking care of how their models will be deployed, whatever the target environment is. On the other hand, enterprises and network providers using ONAP will be empowered to deploy such models, train, test, retrain and redeploy them in their respective networks. Such a unified open-source platform will not only help network providers to onboard and analyze research studies for their corresponding use cases but will also allow researchers to learn about unseen scenarios of a real network that could never be learned through simulated testbeds. As part of our future work, we intend to study, develop and deploy DCAE flows (group of interconnected DCAE service components) by exploring various components of the DCAE Collection Framework and Acumos based ML models, thereby provide fully automated

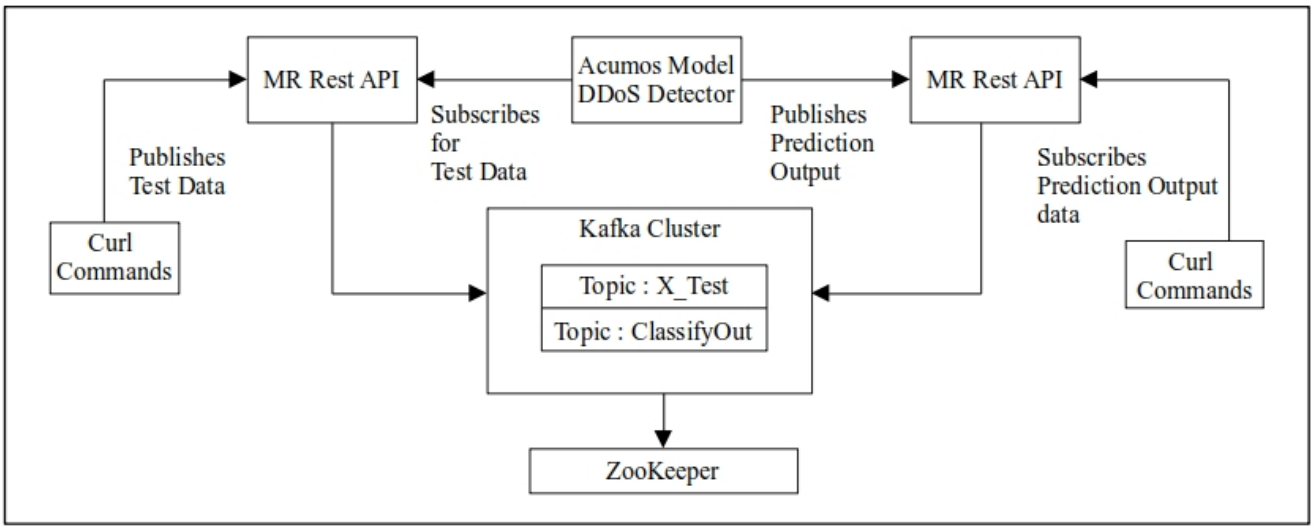

Fig. 3. DDoS Detector running as microservice in the ONAP platform

solutions to different use cases in various networks, including optical networks.

ACKNOWLEDGMENT

We convey our gratitude to the members of both the Acumos Model Management Team and the ONAP-DCAE community for their support and assistance. We also acknowledge ITU-T Focus Group on Autonomous Networks for their interests and collaboration.

REFERENCES

[1] J. Xie et al., "A survey of machine learning techniques applied to Software Defined Networking (SDN): research issues and challenges," in IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 393-430, Firstquarter 2019, doi: 10.1109/COMST.2018.2866942.

[2] N. Dragoni et al., "Microservices: how to make your application scale," In: Petrenko A., Voronkov A. (eds) Perspectives of system informatics, vol 10742, 2017, Available: https://doi.org/10.1007/978-3-319-74313-4_8

[3] ONAP Community (contributed by AT&T), "ONAP Architecture," [Online]. Available: https://docs.onap.org/en/latest/guides/onap-developer/architecture/onap-architecture.html#id1

[4] Acumos Community (contributed by AT&T), "ACUMOS: An open source AI machine learning platform," [Online]. Available: https://www.acumos.org/wp-content/uploads/sites/61/2018/03/acumos_open_source_ai_platform_032518.pdf

[5] M. Radif, A. Alrammahi, "CTR prediction with deep neural networks," Journal of Engineering and Applied Sciences, vol 14, pp. 10560-10568, 2019.

[6] S. Zhao et al., "Packaging and sharing machine learning models via the Acumos AI open platform," 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA, pp. 841-846, 2018, Available: doi: 10.1109/ICMLA.2018.00135.

[7] J.Ye, X. Cheng, J. Zhu, L. Feng, L. Song, "A DDoS Attack Detection Method Based on SVM in Software Defined Network," Security and Communication Networks, vol. 2018, Article ID 9804061, 2018. Available: https://doi.org/10.1155/2018/9804061

[8] Dong Li et al., "Using SVM to detect DDoS attack in SDN network," IOP Conf. Ser.: Mater. Sci. Eng. 466 012003, 2018

[9] Acumos Community (contributed by AT&T), "Acumos: Architecture guide," [Online]. Available: https://docs.acumos.org/en/latest/architecture/intro.html

[10] ONAP Community (contributed by AT&T), "Open Network Automation Platform overview," [Online]. Available: https://docs.onap.org/en/guilin/guides/overview/overview.html#functional-overview-of-onap

[11] ONAP Community (contributed by AT&T), "ONAP platform architecture," [Online]. Available: https://www.onap.org/architecture

[12] F. Slim, F. Guillemin, A. Gravey and Y. Hadjadj-Aoul, "Towards a dynamic adaptive placement of virtual network functions under ONAP," IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)," Berlin, pp. 210-215, 2017, Available: doi: 10.1109/NFV-SDN.2017.8169880.

[13] ONAP Community (contributed by AT&T), "Data Collection, Analytics and Events (DCAE)," [Online]. Available: https://wiki.onap.org/pages/viewpage.action?pageId=1015831

[14] ONAP Community (contributed by AT&T), "DMaaP – Data Movement as a Platform proposal," [Online]. Available: https://wiki.onap.org/pages/viewpage.action?pageId=3247130#:~:text=DMaaP%20is%20a%20premier%20platform,1.

[15] ONAP Community (contributed by AT&T), "OOM with TOSCA and Cloudify," [Online]. Available: https://wiki.onap.org/display/DW/OOM+with+TOSCA+and+Cloudify

[16] Apache Kafka, "A distributed streaming platform," [Online]. Available: https://kafka.apache.org/

[17] AT&T and Linux Foundation, "Acumos DCAE integration," [Online]. Available: https://wiki.onap.org/display/DW/Acumos+DCAE+Integration

[18] Openstack, "The most widely deployed open source cloud software in the world," [Online]. Available: https://www.openstack.org/software/

[19] Kubernetes, "Production-Grade container orchestration," [Online]. Available: https://kubernetes.io/

[20] Acumos Community (contributed by AT&T), "Acumos OneClick / All-in-One (AIO) user guide," [Online], Available: https://docs.acumos.org/en/clio/submodules/system-integration/docs/oneclick-deploy/user-guide.html

[21] ONAP Community (contributed by AT&T), "ONAP on HA Kubernetes Cluster," [Online]. Available: https://docs.onap.org/projects/onap-oom/en/latest/oom_setup_kubernetes_rancher.html#onap-on-kubernetes-with-rancher

[22] S. Sultana, "Acumos/DCAE Integration, ML/AI aided ONAP-DCAE," [Online]. Available: https://extranet.itu.int/sites/itu-t/focusgroups/an/SitePages/Home.aspx

[23] Canadian Institute of Cybersecurity, "NSL-KDD dataset," [Online]. Available: https://www.unb.ca/cic/datasets/nsl.html

[24] ONAP Community (contributed by AT&T), "DCAE MOD architecture," [Online]. Available: https://wiki.onap.org/display/DW/DCAE+MOD+Architecture