Enhancing Cloud Security: A Comprehensive Framework for Threat Mitigation and Policy Implementation

Dr. M. Mohamed Musthafa, Dr.G.Balaji, Mr.S. Noor Mohammed, Mr.Ashir Sha Backer,
Mr. Md Arif Nazam, Mr.R. Ayubkhan., Mr. A. Hussain Fardeen Nasir,
Al-Ameen Engineering College,Erode

Abstract

Cloud computing is not a new technology but rather an evolution of IT infrastructure, transitioning from centralized computing to network-dependent distributed systems. It is widely recognized for its pay-per-use model, elasticity, scalability, ubiquity, and resource availability, making it an essential component of modern enterprises. However, security remains a persistent challenge as organizations migrate to cloud-based environments. Despite advancements in cloud security techniques, concerns regarding data protection, unauthorized access, and system vulnerabilities continue to pose significant risks. This study provides a comprehensive analysis of prevailing threats and weaknesses in cloud computing, emphasizing the need for robust security requirements in cloud services. Additionally, it proposes a Cloud Security Policy framework designed to enhance data protection, access control, and threat mitigation. By assessing the current state of cloud security research, practices, and policies, this study aims to guide practitioners toward more resilient cloud security strategies, ensuring secure and reliable cloud computing environments.

Key words: elasticity, ubiquity, scalability, resource availability, Cloud Computing, security.

1. Introduction

Cloud computing was a service that enables users to rent computational capabilities on-demand, effectively turning computing into a utility [3]. Cloud computing eliminates the need for enterprises to own their own physical equipment and the human work required to maintain it because of this efficient use of computer power. To provide such a solution, a cloud provider aggregates a significant lot of actual hardware [4], which can then be virtualized and made available to customers [5]. Because the quantity of virtual servers

available on demand can be expanded at any time to quickly respond to changing requirements, users do not need to prepare for the resources they require [6].

To summarise, cloud capabilities' elasticity enables for optimal exploitation of computer resources because the quantity of resources can be adjusted to meet actual demand. This diagram depicts the challenges of static resource providing, often known as over and under administration, and how they are addressed via variable cloud resource procurement. Because the capacity is fitted to the peak of the predicted demand, overprovisioning has the disadvantage of paying for underutilised resources during down times. When capability is set to a smaller proportion of peak load times, as in the under provisioning example (Figure 3.1 b), there are insufficient resources to process all user request, resulting in user discontent and, as a result, a decrease in demand. When capability is set to a lower number of peak times, as in the over provisioning example (Figure 3.1 b), there are insufficient resources to process all user request, resulting in user discontent and, as a result, a decrease in overall demand. When Cloud Provisioning is used, however, capability could be dynamically modified to meet demand. This provides a significant cost savings because only the resources required must be rented. As a result, cloud computing uses a pay-as-you-go pricing scheme, which lowers the cost of service process for customers [5].

2. Cloud Computing Architecture

This section, in contrast to the NIST guideline [4,] gives an outline of cloud infrastructure's basic framework. As shown in Figure 1, the design is made up of 4 modular layers: equipment, network, system, and app. Furthermore, based on the cloud application services, this diagram depicts the layers to which a customer has accessibility. The hardware layer includes the cloud system's material assets.

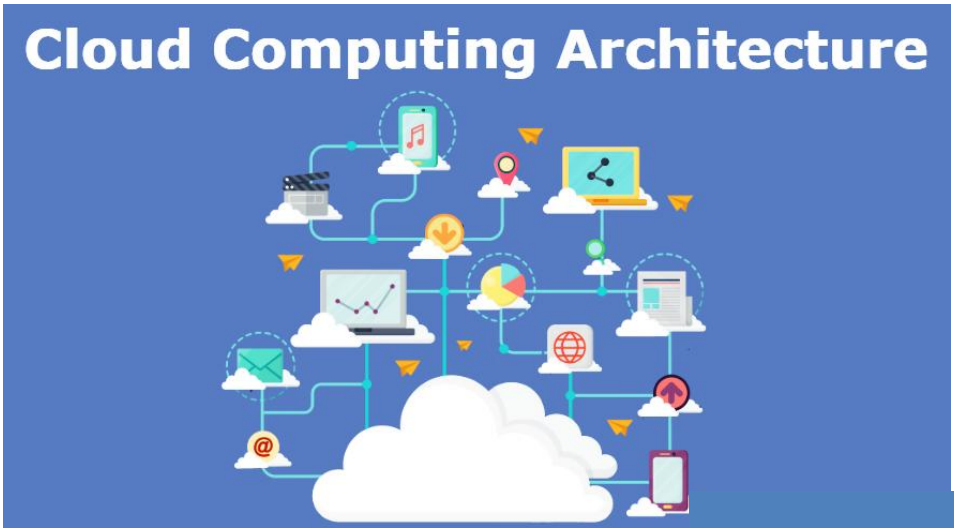

Figure 1: Cloud computing architecture

2.1 Provider Lock-In

Despite the fact that cloud computing provides a convenient approach to access computational power as a utility, some challenges remain unsolved. The provider lock-in, which specifies a supplier lock-in that ties a cloud user to a provider after a cloud service is constructed or established [14], is another one of those issues.

2.2 Interface for Open Cloud Computing

In this thesis, we use the OCCI [17], an OGF [18] standard, to create abstractions of cloud services that we can compare, install, and adjust. In summary, the standard specifies an API and a border protocol that enable for straightforward cloud service control via REST calls. As seen in Figure 2, the OCCI protocol can be deployed alongside any private API by the supplier. From the perspective of a provider, this diagram demonstrates OCCI's position in the public cloud.

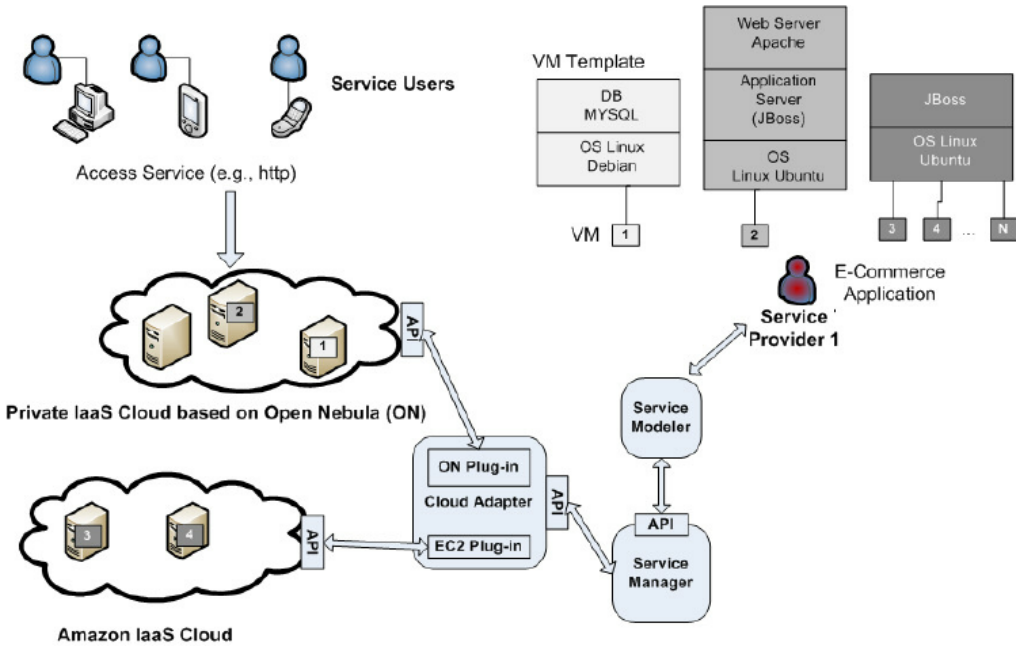

Figure 2: In a provider's architecture, the OCCI API is used.

2.2.1 Core Model

The OCCI Core Framework specifies a model for abstracting real-world cloud services and hence forms the backbone of the specification [1]. The model's elements, in this case, represent individual resources that are handled via REST calls. The OCCI Firm is illustrated in Figure 3.4. The core basis types and the categorization and identification procedures are the two sections of the OCCI Modelling Tool [1]. These two aspects will be examined in depth in the next sections.

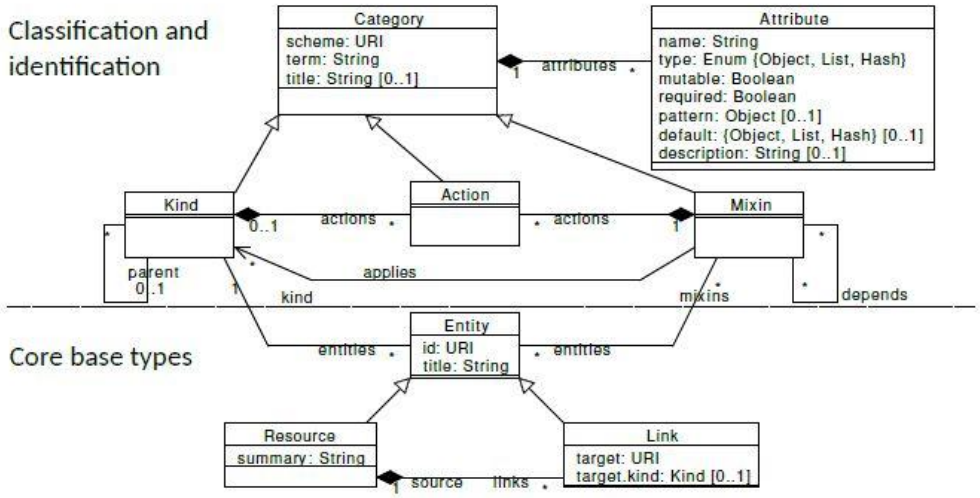

Figure 3: OCCI's Core Model

The components Entity, Asset, and Link make up the fundamental base types. New structures of the Resource component represent idealized real-world resources such as virtual machines, storage, and networks. The source Resource includes a Link element, which provides information about the destination, to define a link between 2 Resources. The abstract Object element, which provides name and id to distinguish those, is inherited by both Resource & Link.

2.2.2 Infrastructure Extension

The infrastructure addition [20] adds particular Entities to the OCCI Core Model that are needed to encapsulate and manage basic IaaS resources like VMs, internet, and memory. Figure 3.5 depicts 3 original Resource kinds and 2 additional Link types as part of the infrastructure expansion. Each type derives from Source or Connection and is given to a named Kind counterpart. Within the Entity type, the Characteristics specified by the Type are represented.

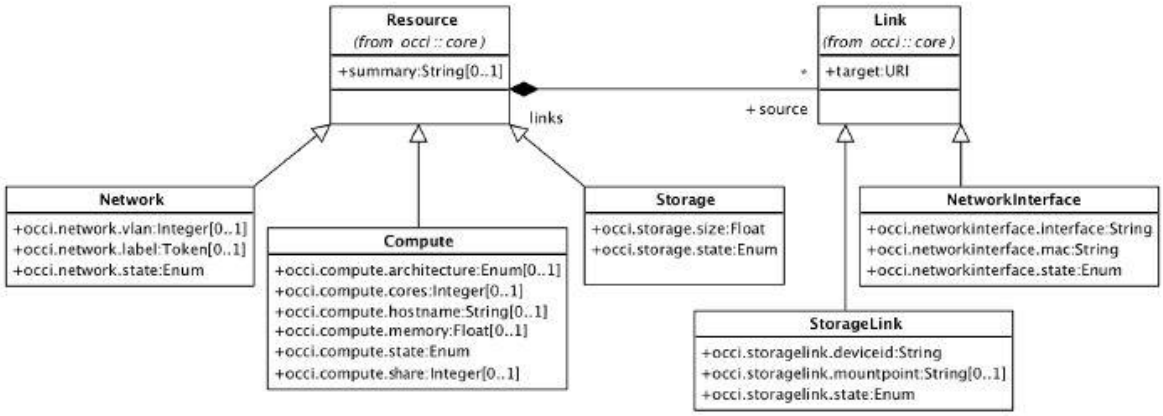

Figure 4: OCCI's infrastructure extension

2.2.3 Platform Extension

The platform module [21] defines classes that describe and assist PaaS resource management. Two Resource kinds and one Link kind are defined in total, as shown in Figure 3.6. In addition, the platform addition identifies 2 Templates that can be used to generate ready-to-use Application settings. The kinds and Frameworks defined by the OCCI framework extension are detailed in the following sections.

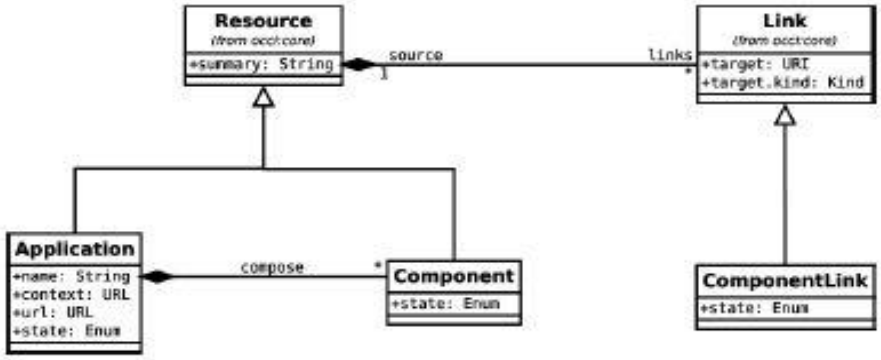

Figure 5:The platform extension of OCCI

Table 1 shows the behaviour of CRUD operations

Path	GET	POST	POST (Action)	PUT	DELETE
Entity sub-type (/compute/1).	Retrieve the Entity.	Partial update of the Entity	Perform an action on the Entity	Create / Update the Entity	Delete the Entity
Entity collection (/compute/1).	Retrieve the Entity collection	Create a new Entity in this collection	Perform actions on the Entity collection	Not defined	Remove all Entities from the collection
Mixin-defined Entity collection (/my_stuff/).	Retrieve a collection of Entity of the given sub-type	Add on Entity to this collection	Perform actions on the Entity collection	Update the Entity collection	Remove all Entities from the collection
Query Interface (/-/)	Retrieve category instances	Add a user-defined Mixin	Not defined	Not defined	Remove a user-defined Mixin

3. Cloud Authentication Attacks

Authentication is a method that assures and verifies that a user's credentials are correct and legitimate. 1 When a user attempts to access information, verification begins. First, the user must demonstrate that he has access permissions and that he possesses the requisite essential characteristic for the verification process. In a public cloud, a user attempts to connect to cloud services by have his own credentials to identify himself and gain access to the cloud services.

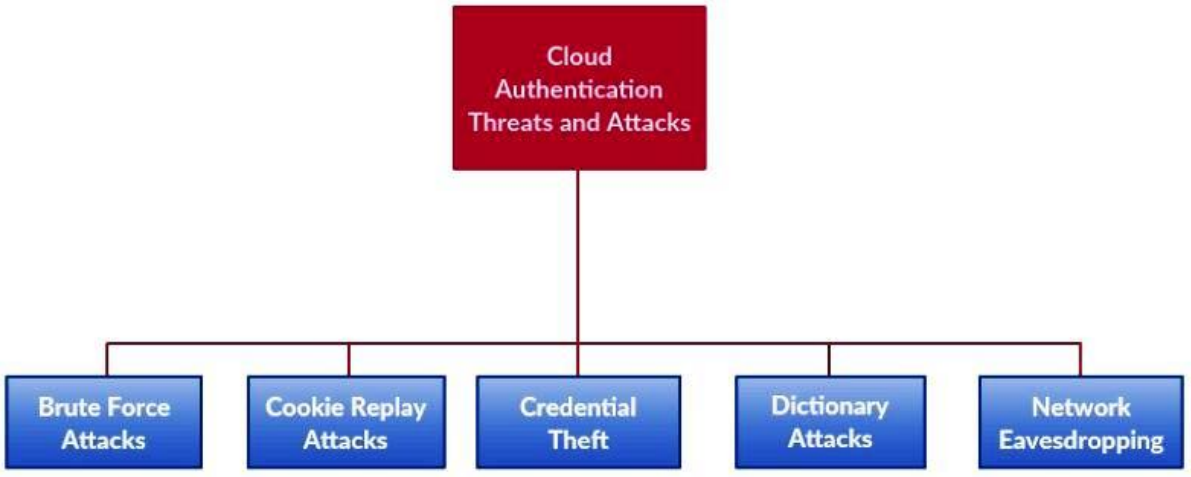

Figure. 6Threats and Attacks Against Cloud Authentication

A protocol incorporating a TTP is employed since the browser cannot produce cryptography acceptable XML tokens to verify the user before reaching cloud services. Microsoft's Passport was a concept for such technologies. It's possible that the browser lacks the necessary passwords, making public login to the server difficult.

3.1. Cloud Malware Injection Attacks

Malicious virtual machines (IaaS) or service implementations (PaaS or SaaS) are injected into the CC network in cloud malware code injection. Through subtle data manipulation, standard channels changes, blockings, and other means, these assaults can result in surveillance. Crackers accomplish this by creating malicious data design modules or virtualization software and integrating them into the CC system. The cracker then deceive the system into treating the harmful services or virtual machines (VMs) as legitimate for the victim. When the assault is successful, the CC system sends legitimate user's request to the rouge system, allowing the adversarial code to run.

3.2. DOS Attacks and Mobile Terminal Security:

Malicious virtual machines (IaaS) or service implementations (PaaS or SaaS) are injected into the CC network in cloud malware code injection. Through subtle data manipulation, standard channels changes, blockings, and other means, these assaults can result in surveillance. Crackers accomplish this by creating malicious data design modules or virtualization software and integrating them into the CC system. The cracker then deceive the system into treating the harmful services or virtual machines (VMs) as legitimate for the victim. When the assault is successful, the CC system sends legitimate user's request to the rouge system, allowing the adversarial code to run.

3.3. Insecure API's

Cloud service providers and software engineers use APIs to enable their clients to communicate with, extract information from, and control cloud services. APIS can be implemented in at least 3 different methods. They could be used to gather logs from a programme, for starters. Second, they could be utilised to make database and storage elements integration 38 easier. Finally, they can be utilised to manage specific cloud resources. APIs are also the primary means by which mobile applications communicate with sites or rear services [85]. They also make it easier for users to authenticate themselves. A network of an online merchant, Moonpig, was broken through a smartphone app, employing static identification, and crackers were able to obtain client information by progressively attempting different APIs.

3.4.Insider Risks in the Cloud Service:

In this situation, the cloudprovider employs an insider. He or she has the potential to harm both the supplier and its customers. Controls exist to mitigate the effects of malicious insider assaults; they are classified into client-side and provider-side remedies. Privacy and availability measures are available on the client side, while hostile insider identification models, recording, and legal binding are available on the supplier side.

3.6. PROBLEMS WITH PRIVACY IN CLOUD COMPUTING

Because a customer's data and business logic should be transferred to cloud servers controlled and managed by cloud providers rather than the customer, privacy is a critical concern in cloud technology.

3.7. Cloud Computing Privacy Overview

Because cloud computing includes multi-tenancy and information sharing, there is a greater danger of privacy and security breaches. When users upload their data to a cloud platform, they lose control over the data's privacy. Given that some firms wish to build their

services while keeping their data private, public cloud is not suitable for privacy. Users' sensitive information is at greater danger of illegal access and disclosure as loads are shifted to shared facilities. Companies have stated their apprehension about storing their applications and data on systems that are not located on their premises.

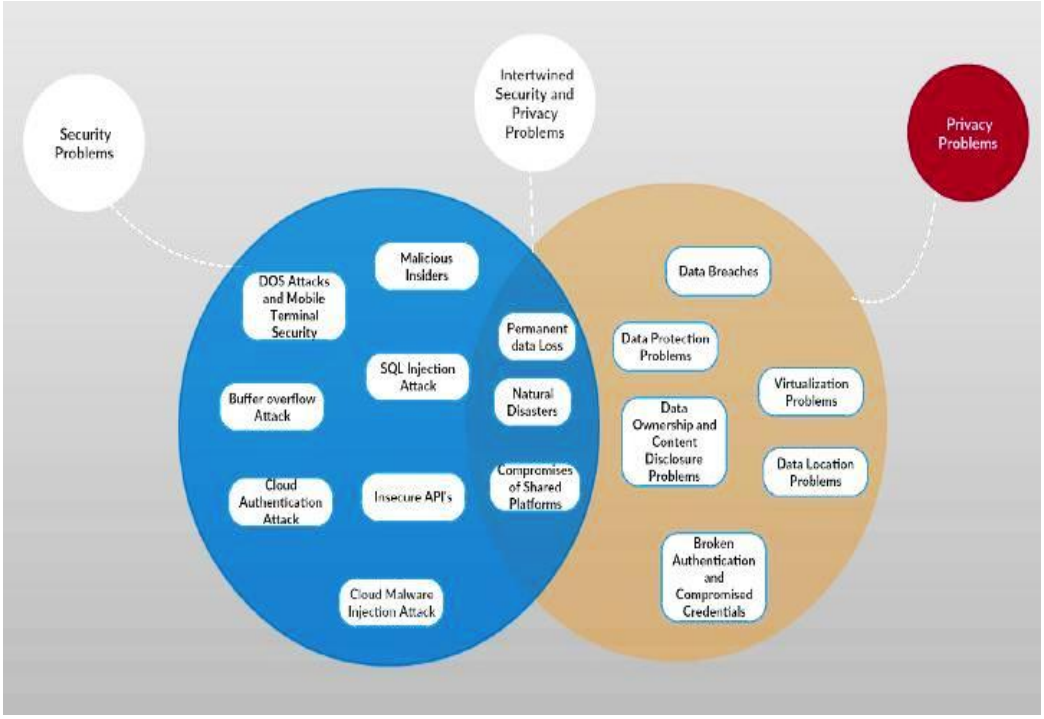

Figure 7. In CC, there are security-only, privacy-only, and intertwined security-privacy issues.

4. Conclusions:

Cloud computing is a fascinating new technology that has the potential to help organisations save money while increasing productivity. Regardless of the fact that Cloud Hosting was already implemented and used in production environments, Cloud Security is still very much in infancy, and further research is needed. A number of recent papers have addressed broad concerns about Cloud Security and Privacy, and experts have highlighted a number of critical issues for dependable Cloud Computing Environment. To ensure corporate continuity, the SaaS provider must have a variety of security safeguards in place. As a result, the most important conclusion from this study is the creation of a Trusted Cloud Provider that achieves the requisite level of confidence while lowering the risk of user information being exposed.

References:

[1] K. Ashton, “That ‘Internet of Things’ Thing - RFID Journal,” RFiD J., vol. 22, no. 7, pp. 97–114, 2009.

[2] Z. Pang, et al., “Design of a terminal solution for integration of in-home health care devices and services towards the Internet-of-Things,” Enterp. Inf. Syst., vol. 9, no. 1, pp. 86–116, 2015.

[3] G. Broil, M. Paolucci, M. Wagner, E. Rukzio, A. Schmidt, and H. Hußmann, “Perci: Pervasive service interaction with the internet of things,” IEEE Internet Comput., vol. 13, no. 6, pp. 74–81, 2009.

[4] M. Darianian and M. P. Michael, “Smart home mobile RFID-based internet-of-things systems and services,” in Proc. 2008 Int. Conf. Adv. Comput. Theory Eng. (ICACTE), pp. 116–120, 2008.

[5] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of things for smart cities,” IEEE Internet Things J., vol. 1, no. 1, pp. 22–32, 2014.

[6] L. Da Xu, W. He, and S. Li, “Internet of things in industries: A survey,” IEEE Trans. Ind. Informatics, vol. 10, no. 4, pp. 2233–2243, 2014.

[7] J. Rivera and R. Van der Muelen, “Gartner says the internet of things installed base will grow to 26 billion units by 2020,” Gartner, 2013. [Online]. Available: https://www.gartner.com/doc/2625419/forecast-internet-things-worldwide-. [Accessed: 26-Nov-2015].

[8] A. Klubnikin, “Internet of Things: How Much Does it Cost to Build IoT Solution?,” [Online]. Available: http://r-stylelab.com/company/blog/it-trends/internet-of-things-how-muchdoes-it-cost-to-build-iot-solution. [Accessed: 01-Nov-2016].

[9] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (IoT): A vision, architectural elements, and future directions,” Futur. Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.

[10] F. Li, M. Vögler, M. Claeßens, and S. Dustdar, “Efficient and scalable IoT service delivery on cloud,” in Proc. IEEE CLOUD, pp. 740–747, 2013.

[11] S. Nastic, S. Sehic, M. Vögler, H. L. Truong, and S. Dustdar, “PatRICIA – A novel programming model for IoT applications on cloud platforms,” in Proc. IEEE 6th Int. Conf. Serv. Comput. Appl. (SOCA), pp. 53–60, 2013.

[12] F. Khodadadi, R. N. Calheiros, and R. Buyya, “A data-centric framework for

development and deployment of internet of things applications in clouds," in Proc. 2015 IEEE 10th Int. Conf. Intell. Sensors, Sens. Networks Inf. Process., pp. 1–6, 2015.

[13] M. Yuriyama and T. Kushida, "Sensor-cloud infrastructure physical sensor management with virtualized sensors on cloud computing," in Proc. 13th Int. Conf. Network-Based Inf. Syst. (NBiS), pp. 1–8, 2010.

[14] S. Nastic, S. Sehic, D. H. Le, H. L. Truong, and S. Dustdar, "Provisioning software-defined IoT cloud systems," in Proc. 2014 Int. Conf. Futur. Internet Things Cloud (FiCloud), pp. 288–295, 2014.

[15] R. Cortés, X. Bonnaire, O. Marin, and P. Sens, "Stream processing of healthcare sensor data: Studying user traces to identify challenges from a big data perspective," Procedia Comput. Sci., vol. 52, pp. 1004–1009, 2015.