Fog Orchestrator as an Enabler for Security in Fog Computing: A Review

Nhlakanipho C. Fakude
Department of Computer Science
University of Zululand
Private Bag X1001, KwaDlangezwa, 3886, South Africa
ncfakude30@gmail.com

Paul Tarwireyi
Department of Computer Science
University of Zululand
Private Bag X1001, KwaDlangezwa, 3886, South Africa
ptarwireyi@gmail.com

Matthew O. Adigun
Department of Computer Science
University of Zululand
Private Bag X1001, KwaDlangezwa, 3886, South Africa
profmatthewo@gmail.com

Adnan M. Abu-Mahfouz
Council for Scientific and Industrial Research (CSIR)
Pretoria 0184, South Africa
a.abumahfouz@ieee.org

***Abstract*—Internet of Things (IoT) aims to bring every object such as smart cameras, wearable devices, environmental sensors, home appliances, and vehicles online. These "*Things*" generate an unprecedented amount of data and transmit it to the cloud for long-term processing and because existing data processing or analytics approaches are designed to deal with massive data and not real-time data, having millions of "*Things*" generating and transferring data to the cloud is neither scalable nor suitable for real-time decision making. Therefore, the current infrastructure will not be able to handle the massive volume of data that will be generated by these devices, hence a new paradigm known as Fog Computing has been proposed. Fog computing extends the cloud platform model by providing computing resources at the edge of the network which results in better performance. However, researchers have raised challenges such as security and privacy, which arise from IoT-based Fog computing environments. Although technologies and solutions enabling connectivity and data delivery are growing rapidly, not enough attention has been given to the security of these computing paradigms and the associated IoT devices. Hence, this paper investigates and compare Fog Orchestrators that enable security in fog computing and further investigate the security techniques used in IoT-based Fog computing environments. This discussion shows that due to better performance brought by Fog Orchestrators, security and privacy models can be implemented in IoT-based fog environments.**

Keywords— Internet of Things (IoT), Fog Computing, Fog Orchestrator, Security and Privacy Model

I. INTRODUCTION

The interconnection of "*Things*" has grown drastically due to the number of devices being deployed and connected to the internet and it has been reported that the number exceeded the world's population in the year 2010 and presently (2019), 26.66 billion devices are connected and by the year 2025, 1 trillion deployments of IoT devices are expected [1], [2]. Fog computing has been proposed to minimize latency, network usage, energy consumption, and ultimately reduce severe consequences of failure in the Internet of Things (IoT).

Fog computing is a new and modern computing paradigm that complements the cloud computing and has recently emerged as a new paradigm that extends the computing infrastructure from the center to the edge of the network. Fog computing is one of the three different Edge Computing implementations (Fog computing, Cloudlet, and Mobile Edge Computing) and it is a decentralized computing paradigm in which substantial amount of computing and storage are carried by edge devices locally [3]. Fog computing enables minimization of data transmission overheads, lowers latency, and provides a platform to enforce security and privacy at the edge of the network [4]. The Fog computing paradigm is largely motivated by the continuous growth of the IoT and it opens doors to innovations that build new types of interaction among things or objects, and humans while enabling the realization of smart cities, infrastructures, and services for enhancing the quality of life and use of resources.

Literature has opened up about the several challenges that are confronting the use of Fog computing among which are the concern about security and privacy of IoT devices in a Fog computing environment [4]. Organizations utilizing Fog computing allow IoT devices to transmit and store confidential data to the cloud through fog nodes and in turn, suffer from the lack of proper and efficient security measures implemented in their fog computing architectures [5].

The implementation of security in a fog-computing environment provides confidentiality, data integrity, and availability but any security integration comes at a cost. Many security solutions affect the performance of the system; i.e. more resources are needed to perform the security processes deployed. Therefore, the introduction of a security model negatively affects the overall performance of the IoT-based Fog computing environments. However, researchers have proposed orchestration as a solution to performance issues.

An orchestrator describes the automated arrangement, coordination, resource management and it is often discussed as having an inherent intelligent or even implicitly automatic control. A Fog Orchestrator (FO) acts as a controller deployed on a workstation or cloud datacenter and across all entities based on global information. Fog Orchestrator provides the centralized arrangement of the resource pool, mapping applications with specific requests and providing an automated workflow to physical resources, workload execution management, and time-efficient directive generation to manipulate specific objects [6].

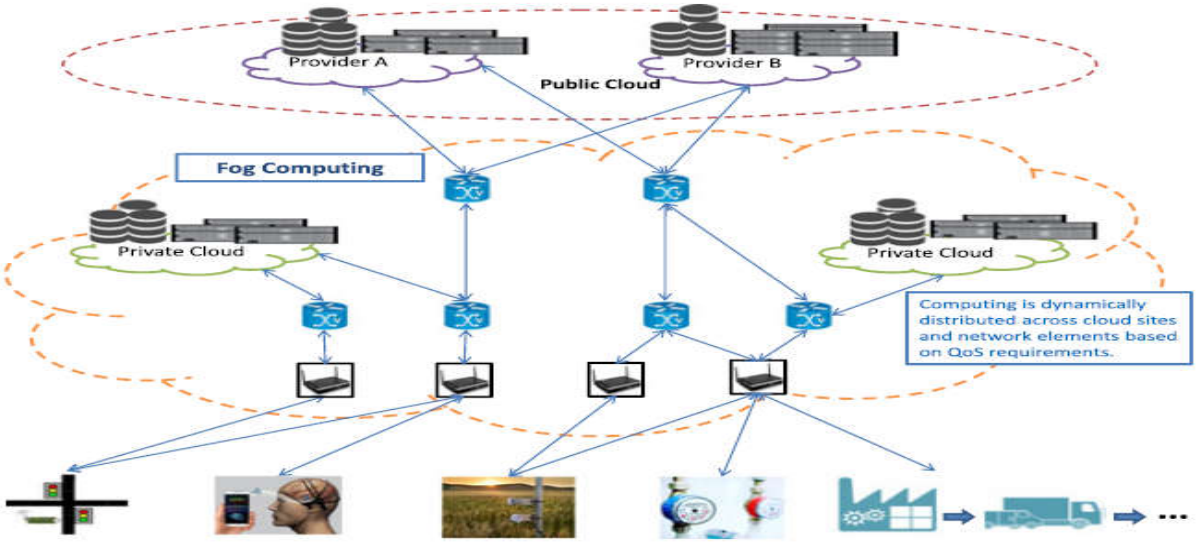

Fig. 1. IoT based Fog Computing Environment [1]

This paper presents a review related to emerging and enabling technologies with main focus on Fog computing which is envisaged to support the exponential traffic growth in IoT. The challenges and open research directions are also presented. The rest of this paper is summarized as follows; section II. Fog Computing Overview, section III. Fog Orchestrators, section IV. Security Models in Fog Computing, and lastly discussions and conclusion.

II. Fog Computing Overview

An IoT based Fog computing environment is an architecture in which end devices (sensors or mobile devices), fog nodes such as fog devices (gateways) are located at the edge of the network where there is a limited amount of resources, and a remote tier of distant cloud servers, which typically have infinite resources. This architecture has the benefits of computation offloading from end devices to the public cloud while limiting the use of the cloud whose higher latency could negatively impact the user experience.

The IoT based Fog computing paradigm enables the seamless convergence of infrastructure stretching from the public cloud to devices on the edge of the network (where intermediate devices like ISP gateways, cellular base stations, and cloud deployments are included) into a continuum of resources, to be provisioned to multiple tenants for hosting applications (see Fig. 1) [1], [7]. The Fog environment provides a platform for filtering and analysis of the data generated by end devices (sensors) by using resources of the edge devices or fog devices.

III. Fog Orchestrators

Researchers have proposed many Fog Orchestrators for IoT-based fog computing architectures and in [8], the authors have mentioned scheduling, path computation, discovery and allocation, interoperability, latency, prediction and optimization, security and privacy as some of the main challenges that need to be addressed by a Fog Orchestrator. There are immediate and major challenges that arise from a fog environment that is enabled with a Fog Orchestrator and these challenges are distributed infrastructure protection, identity lifecycle and cryptographic key management (i.e. secure generation, distribution, exchange, storage, and replace of credentials and keys) [8].

A. Fog Orchestrator in 5G-enabled Smart Cities

A Fog Orchestrator has been proposed to attack the security challenges of Fog computing through a centralized system. The authors proposed a Fog computing framework, which enables autonomous management and orchestration functionalities in 5G-enabled Smart Cities. Their approach followed the guidelines of the European Telecommunications Standards Institute (ETSI) NFV MANO Architecture. The proposed framework aims to deal with application service placement problem in Smart Cities. The authors' approach enables security integration as it follows the ETSI oneM2M organization where an end-to-end high-level architecture has been designed for Machine-to-Machine (M2M) communications. The proposed design enables device management and contains security functionalities [9]. Zen *et al.* mentioned that a fog orchestrator is a centralized controller at a conceptual level and raised the issue of single point of failure in fog computing architectures [6]. Hence the major drawback of the study conducted by Santos *et al.* [9] is the Fog Orchestrator being a centralized system which could result in a single point of failure.

B. Fog Service Orchestration Architectures

Other researchers have identified key challenges in the development of a Fog Orchestrator to support the Internet of Things (IoT), including how they affect the tasks that a Fog Service Orchestrator should perform [10]. Their work presented a review of the main challenges that impair the migration of the orchestration mechanisms from the cloud to the fog. The work also discussed the following different versions of Fog Service Orchestration architectures:

- SORTS
- SOAFI
- ETSI IGS MEC

- CONCERT

The authors described a Fog Orchestrator as a centralized entity that organizes the Fog nodes into Logical Infrastructure and through this grouping; it is possible to create the hierarchy of capacity and objectives within the framework. It has also been mentioned that to improve the performance of a fog computing environment, data needs to be aggregated at the Fog level where Fog Nodes are located before being sent to the global cloud, thus the new solution considered data aggregation and pre-processing.

The challenges reviewed by Velasquez *et al*. resulted in the realization of orchestration importance but since the fog orchestrator is a centralized entity, single point of failure adds to the challenges and before Fog Nodes transfer data to the cloud, the sensors (IoT devices) should transmit raw data to the Fog layer, hence attacks can be performed between the sensor and fog layer [8], [9].

C. *Fog-enabled Orchestration for IoT Services*

An overview of the core issues, challenges and future directions in Fog-enabled orchestration for IoT services were provided in [6] and the authors provided scenarios on which Fog Orchestration can be applied to IoT services and have mentioned that a Fog Orchestrator is a centralized controller only at a conceptual level and might be implemented in a distributed and fault-tolerant fashion without introducing a single point of failure.

IoT applications deployed within Fog computing systems consist of the Cloud, Fog Node, and *"Things"*, and in this context the authors have defined a Fog Node as an equipment or middleware used by a Fog Orchestrator and it serves as an agent that collects data from a set of IoT devices (sensors, actuators) which is transmitted to a centralized computing system (FO) that locally processes and caches data. This work does not provide any security approaches or techniques that can be followed in the deployment of the proposed Fog Orchestrator

D. *Service Orchestration for Fog-enabled Infrastructures*

Moreover, researchers have proposed an orchestration architecture for Fog computing environments where Fog Nodes are used for computation and storage and these computational nodes must be able to communicate with a variety of devices, sensors, and actuators and the proposed approach offers services based on global information gathered and processed or filtered locally [11].

Orchestration allows Fog Nodes to be programmable in the Fog infrastructure and the authors' work conforms to the ETSI) NFV Management and Orchestration (MANO). The proposed orchestrator solution abstracts the Virtualization/Containerization software running in the Node (Docker, Xen, etc.), not the abstraction of the virtualized infrastructure (e.g. OpenStack) [11]. The difference between the proposed approach and the MANO approach is that the nodes virtualization underlying system is abstracted whereas on the MANO approach infrastructures are virtualized.

The proposed Orchestrator and Infrastructure Manager fit in the Software View, which contemplates Node Management, Application Services, and support. Hence, security was one of the requirements to the proposed orchestrator.

E. *ETSI NFV MANO Reference Architecture*

The ETSI NFV MANO is said to be clean and flexible and it was initially conceived for VNF Orchestration, and due to its characteristics, it has been considered adapted to handle other kinds of services. Various researchers have borrowed some characteristics from the ETSI MANO and they have considered the different Fog computing environment needs. ETSI MANO is intended to deal with computing nodes that can vary on hardware (CPU, memory, network) and software specifications (Hypervisor, Operating System, etc.), while in Fog environments, physical devices (e.g. sensors and actuators) have capabilities needed by an orchestrator [11].

F. *Mobile Edge Computing Reference Architecture*

In the field of Mobile Edge Computing, the ETSI MEC Reference Architecture conceives an Orchestrator that very similar requirements to the IoT based Fog computing environment [12]. As of this writing, the community is still discussing the differences and similarities of both Mobile Edge Computing orchestration and the orchestration of Fog computing [13].

IV. SECURITY IN FOG COMPUTING

There are many security and privacy issues in the Fog computing paradigm that have been discussed by researchers and authentication at different fog devices (e.g. gateways) has been pointed as one of the major security challenges in IoT environments. Several security attacks have been performed and the authors studied a typical man-in-the-middle attack to investigate the features of the attack by examining the memory consumption and CPU of a fog device in a stealthy test environment of the fog computing paradigm and the study showed that since IoT can play a central role in delivering a rich portfolio of services effectively and efficiently to end-users, it poses more major challenges such as Authentication, Trust, Rogue Node Detection, privacy, Access Control, Intrusion Detection, Data protection, and many more security and privacy issues [14]. In addition to the security challenges faced by IoT-based fog computing environments, the authors in [15] discussed the relationship between cloud computing and fog computing and have addressed the security issues of cloud computing which forms part of the security challenges faced by fog computing.

Fig. 2 shows the three core layers of Fog computing; sensor layer, fog layer, and the cloud layer. The sensor layer contains IoT devices (e.g. sensors and actuators), the fog layer provides computation and storage resources to the sensor layer, and finally, the cloud layer contains unlimited computing and storage resources. Having seen from Fig. 2 that the sensor, fog, and cloud layers communicate via wireless links, the fog computing architecture becomes susceptible to link attacks such as; data tampering, eavesdropping, man-in-the-middle, message distortion, and denial of service (DoS)[6].

Additionally, fog computing allows sensor devices to transmit raw data into the fog layer where each Fog Node will process the data and perform data analysis operations in

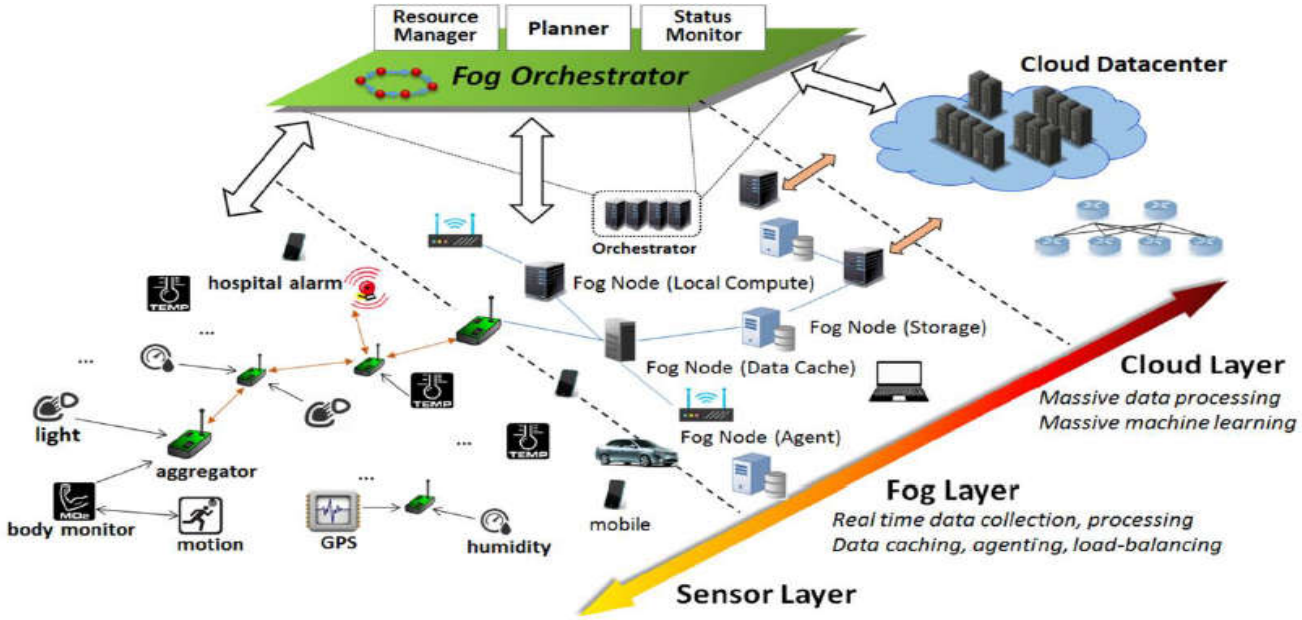

Fig. 2. IoT-based Fog Computing Architecture with Fog Orchestrator [16]

a timely manner, hence that opens a door for attackers to intercept the raw data before it reaches the fog layer [9]. Researchers have done work in fog computing security challenges and have proposed and implemented security solutions to the arising security issues face by IoT-based fog computing environments. issues.

A. *Security Through Encryption*

Encryption has been the most common form of security in the modern era and authors have proposed a security model for the IoT-based fog computing environment in which security is achieved through encryption [2]. The authors discussed the correlation between cloud computing and fog computing and they have opted to use the AES algorithm to encrypt data in the fog environment. Fog devices need to serve end devices through wireless connections hence a secure communication model is essential. One of the major drawbacks of this study is the cost of encryption as mentioned in terms of computation. Fog nodes have to process encrypted data and send responses to actuators and without the help of a fog orchestrator, the task becomes difficult hence bottlenecks and high latencies will be introduced if this model is deployed into an IoT-based fog computing environment.

B. *Policy-Driven Security Management*

Dsouza *et al.* have proposed a policy-based service in which the fog computing architecture is made up of three core components; Internet of Things (IoT) Verticals, Orchestration Layer, and Abstraction Layer and each layer is said to have both virtual and physical components which contribute to the efficient and dynamic functionality of a fog system [17]. The orchestration layer supports data aggregation, decisions, data sharing and migration, and policy management for the fog computing environment. Dsouza *et al* defined a Fog Node as having a primary focus of facilitating seamless and uniform resource management including management of computation, networking, and storage allocation of each node.

Bonomi *et al.* [18], proposed several service orchestration layer components including foglet software agent, distributed databases, policy-based service orchestration, and scalable bus and have introduced a policy-based orchestration framework which Dsouza *et al.* extended by defining existing framework and proposing a policy-based security management for the fog computing paradigm [17]. The concept of policy collaboration as discussed by Dsouza *et al.* is introduced with the goal of supporting secure sharing and communication in a distributed environment. The proposed model by Dsouza *et al.* categorizes requirements into three primary nom-functional; operational requirements, network requirements, and security requirements which focuses on authentication and authorizing access requests between various fog components and smart devices as well as ensuring that policy-specifications are met for multi-tenant applications in the fog computing environment.

C. *Intrusion Detection Systems for Fog Computing*

Security can be provided to IoT-based fog computing through intrusion detection systems and Hosseinpour *et al.* proposed an intrusion detection system (IDS) to tackle cyber threats in logistic systems [19]. Safety and security of monitoring a physical environment in IoT applications such as cyber-physical systems are a critical issue that are mostly underestimated in recent and current studies.

Actuators can be a point of the physical environment in which cyber-attacks are performed, hence the authors proposed a solution which takes into consideration the resource constrained devices in IoT, hence light approaches need to be undertaken to ensure the quality of service (QoS) and feasibility of such security measures. Silent attacks require constant and behavioral analysis of the systems' components and communication to be detected, therefore, precise and swift safety monitoring and intrusion detection system are important in IoT-based logistic systems. One major drawback of the work in the proposed IDS by Hosseinpour *et al.* is the usage of old datasets and modern

datasets are mostly designed for IDS models in the cloud platform [19].

Fog is a decentralized platform which is capable of processing and operating data locally and can be deployed in heterogeneous hardware which makes it ideal for IoT applications. Intrusion Detection Systems (IDSs) are an integral part of any security system and due to the resource limitations or constraints of fog and IoT devices, lightweight IDS are highly desirable, hence, Khater *et al*. [20], proposed a lightweight IDS that is realized by machine learning techniques enabled by orchestration.

The proposed IDS model was tested using ADFA-LD dataset in Raspberry Pi, which in their experiment acted as the Fog device. Hosseinpour *et al*. found out that power consumption is one of the key factors affecting IDS models in fog and IoT environments, hence the authors have conducted experiments and chose CPU time and energy consumption as one of the major performance metrics in evaluating the proposed IDS model [19]. Having considered CPU time and energy consumption, other performance metrics in IoT-based fog computing environments should be considered as well due to the dynamicity of the paradigm and such metrics are latency and network usage which this study did not fully address.

TABLE I. SECURITY IN FOG COMPUTING

Security Model	**Security in IoT-based fog computing**		
	Techniques	***Orchestration***	***Performance metrics***
Security Through Encryption [2]	Advanced Encryption Standard (AES)		Encryption/decryption time, Utilization of memory, Response time
Policy-Driven Security Management [17]	Policy management framework: Policy Decision Engine, Application Administrator, Policy Resolver, Policy Repository, Policy Enforcer	Extension of policy-based orchestration framework [18]	Light traffic load, and Heavy traffic load
Lightweight Intrusion Detection System (IDS) [19]	Artificial Immune System (AIS), Machine learning		False Positive Rate, True Positive Rate, Accuracy, Recall, and Precision
Lightweight Perceptron-Based IDS [20]	Vector Space representation using Multilayer Perceptron model (MLP), Machine learning		Recall, F-Measure, Accuracy, CPU Usage, Testing Time, Energy Consumption

Table 1, shows the different security approaches present in the fog computing environment and most of the techniques are not based on orchestration, i.e. these security models do not take advantages of orchestration (fog orchestrator to be exact). From table 1, the techniques used by the proposed security models have been shown as well as the performance metrics used to evaluate the performance of the models. From literature, energy consumption and latency are some of the vitally important performance metrics in the IoT-based Fog computing paradigm and none of the two have been evaluated on the proposed security models [1]. The grow of the Internet of Things will result in a more complex ecosystem where detection of intrusions and attacks will be difficult to achieve, hence having a conceptual centralized entity (Fog orchestrator) which holds a global overview of the network will help in the design of better security models such as IDS, encryption-based techniques while improving the performance of the environment [5][9].

V. DISCUSSION

Fog computing is a decentralized computing paradigm in which data is processed and stored between the source of origin and global cloud infrastructure. This results in enhanced service quality to IoT devices or mobile device, enhanced efficiency to the network, and enhanced location awareness, hence the performance is enhanced in terms of latency, network usage, and energy consumption of IoT devices when transmitting data to the cloud. Furthermore, data transmission overheads are minimized and subsequently, the fog computing architecture improves the performance of computing at the edge of the network as well as the cloud platforms by reducing the requirement to process and store large volumes of superfluous data [4].

The adoption of fog computing as discussed by Butun *et al*. [21], brought advantages such as reduced costs, reduced delay, agile responses, and provides better performance for IoT-based fog computing environments. The major drawback of security implementation in fog computing is the extra load introduced to the system, i.e. security bring an extra burden to the IoT environment (e.g. processing and memory storage), and that results in bad overall performance for the IoT-based fog computing environment. Hence researchers have proposed fog orchestration to improve the performance of IoT systems.

The introduction of a Fog Orchestrator to an IoT-based fog computing environment lays a platform for researchers to integrate security models that do not negatively impact the performance of the IoT environments. With the emerging and promising fog computing orchestration, there exist possibilities and opportunities in which security and privacy models can be implemented. Since network attacks increase as the number of IoT device deployments increase, improvements need to be a major priority to catch up with these security challenges.

Fog Orchestrator not only improves the performance of fog computing, but it also adds an extra layer which acts as the controller of the whole architecture, i.e. FO holds the entire overview of the fog computing networking, which provides possibilities of implementing various security, resource scheduling and management, and system monitoring. This paper explored fog orchestrators which enable security mechanisms to be realized and we envision a security model in IoT-based fog computing environment which will provide data confidentiality, integrity, non-repudiation, and availability across the sensor, fog, and cloud layers.

VI. Conclusion

This paper explored the security challenges faced by IoT-based fog computing environments. Current techniques used in the security of IoT devices were discussed and categorized. The principle of Fog Orchestration was introduced and security protocols which currently used orchestration to provide security and privacy to IoT based systems were discussed. Although the idea of Fog Orchestrator is promising, the community is still working on improvements and from the reviewed work, there has not been a standard and secured Fog orchestrator yet, therefore, work still needs to be done to create and develop standardized methods of security and privacy within the IoT-based fog computing paradigm.

This paper went on to explore fog orchestrators that support security functionalities while also catering for better performance. The study raised the fact that performance metrics such as latency, network usage, and energy consumption should be of significance when evaluating the performance of an IoT-based security model in fog computing. The introduction of a Fog Orchestrator to an IoT-based fog computing environment lays a platform for researchers to integrate security models that will positively impact the performance of the IoT environment. Hence, this paper proposes that security techniques in fog computing should take the advantages of orchestration in developing security models which will provide confidentiality, data integrity, and availability across the sensor, fog, and cloud layers.

Acknowledgment

The authors acknowledge the funds received from the industry partners: Council for Scientific and Industrial Research (CSIR), South Africa in support of this research.

References

[1] H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh, and R. Buyya, "iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments," *Softw. - Pract. Exp.*, vol. 47, no. 9, pp. 1275–1296, 2017.

[2] A. Vishwanath, R. Peruri, and J. (Selena) He, "Security in Fog Computing through Encryption," *Int. J. Inf. Technol. Comput. Sci.*, vol. 8, no. 5, pp. 28–36, 2016.

[3] K. Dolui and S. K. Datta, "Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing," *GIoTS 2017 - Glob. Internet Things Summit, Proc.*, 2017.

[4] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions," *J. Cloud Comput.*, vol. 6, no. 1, 2017.

[5] I. Stojmenovic and S. Wen, "The Fog Computing Paradigm: Scenarios and Security Issues," *Proc. 2014 Fed. Conf. Comput. Sci. Inf. Syst.*, vol. 2, pp. 1–8, 2014.

[6] Z. Wen, R. Yang, P. Garraghan, T. Lin, J. Xu, and M. Rovatsos, "Fog orchestration for IoT Services: Issues, Challenges and Directions," *IEEE Internet Comput.*, vol. 21, no. 2, pp. 16–24, 2017.

[7] R. Mahmud and R. Buyya, "Modeling and Simulation of Fog and Edge Computing Environments Using iFogSim Toolkit," *Fog Edge Comput.*, pp. 433–465, 2019.

[8] D. F. A. Karima Velasquez, David Perez Abreu , Marcio R. M. Assis, Carlos Senna, E. M. Luiz F. Bittencourt, Nuno Laranjeiro, Marilia Curado, Marco Vieira, and and E. Madeira, "Fog orchestration for the Internet of Everything: state-of-the-art and research challenges," *J. Internet Serv. Appl.*, vol. 2017-Janua, no. 14, p. 23, 2018.

[9] J. Santos, T. Wauters, B. Volckaert, and F. de Turck, "Fog computing: Enabling the management and orchestration of smart city applications in 5G networks," *Entropy*, vol. 20, no. 1, 2018.

[10] K. Velasquez *et al.*, "Service orchestration in fog environments," *Proc. - 2017 IEEE 5th Int. Conf. Futur. Internet Things Cloud, FiCloud 2017*, vol. 2017-Janua, pp. 329–336, 2017.

[11] M. S. De Brito *et al.*, "A service orchestration architecture for Fog-enabled infrastructures," *2017 2nd Int. Conf. Fog Mob. Edge Comput. FMEC 2017*, pp. 127–132, 2017.

[12] ETSI GS MEC, "MEC - Framework and Reference Architecture," vol. 1, pp. 1–18, 2016.

[13] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog Computing: A Taxonomy, Survey and Future Directions," 2016.

[14] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," *IEEE Internet Comput.*, vol. 21, no. 2, pp. 34–42, 2017.

[15] M. Chen, Y. Qian, J. Chen, K. Hwang, S. Mao, and L. Hu, "Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing," *IEEE Trans. Cloud Comput.*, vol. XX, no. c, pp. 1–1, 2016.

[16] Z. Wen, R. Yang, P. Garraghan, T. Lin, J. Xu, and M. Rovatsos, "Fog orchestration for internet of things services," *IEEE Internet Comput.*, vol. 21, no. 2, pp. 16–24, 2017.

[17] C. Dsouza, G. J. Ahn, and M. Taguinod, "Policy-driven security management for fog computing: Preliminary framework and a case study," *Proc. 2014 IEEE 15th Int. Conf. Inf. Reuse Integr. IEEE IRI 2014*, pp. 16–23, 2014.

[18] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, "Big Data and Internet of Things: A Roadmap for Smart Environments," vol. 546, pp. 169–186, 2014.

[19] T. Hosseinpour, Farhoud; Vahdani Amoli, Payam; Plosila, Juha; Hämäläinen and H. Tenhunen, "An Intrusion Detection System for Fog Computing and IoT based Logistic Systems using a Smart Data Approach," *Int. J. Digit. Content Technol. its Appl.*, vol. 10, no. 5, pp. 34–46, 2016.

[20] B. Sudqi Khater, A. Abdul Wahab, M. Idris, M. Abdulla Hussain, and A. Ahmed Ibrahim, "A Lightweight Perceptron-Based Intrusion Detection System for Fog Computing," *Appl. Sci.*, vol. 9, no. 1, p. 178, 2019.

[21] I. Butun, A. Sari, and P. Österberg, "Security Implications of Fog Computing on the Internet of Things," no. 20201010, 2018.