Position Papers of the Federated Conference on Computer Science and Information Systems pp. 69–73
DOI: 10.15439/2019F348
ISSN 2300-5963 ACSIS, Vol. 19

A Fog Computing Architecture for Security and Quality of Service

Bruno Nunes Barreto
Federal University of Sergipe
Av. Marechal Rondon, s/n,
Sao Cristovao, Sergipe, Brazil
Email: bnbarreto@gmail.com

Alexandre Rezende de Sa
Federal University of Sergipe
Av. Marechal Rondon, s/n,
Sao Cristovao, Sergipe, Brazil
Email: alexandresa@ufs.br

Admilson de Ribamar Lima Ribeiro
Federal University of Sergipe
Av. Marechal Rondon, s/n,
Sao Cristovao, Sergipe, Brazil
Email: admilson@ufs.br

***Abstract*—The Fog Computing paradigm is an emerging architecture and focuses on optimizing resources for the Internet of Things environment, bringing to the Edge, Cloud's characteristics. The demand generated by the number of possible devices in this network attracts problems related to quality of service, security, among others, attracting researchers from the most diverse areas. In our work, in addition to performing a study on selected works in a mapping process, detecting trends in the use of Fog architectures. The main contribution is presented by a security-based Fog Computing architecture using QoS for scalable environments with Docker containers for orchestration and deployment of security with SDN.**

I. Introduction

THE TECHNOLOGICAL evolution of embedded equipment has enabled virtual communication with certain objects so that we can manage and operate them at a distance through the Internet. With a finality of increase the interactional capacity in systems, a new paradigm called generically Internet of Things (IoT) has been emerging [1].

Through the integration of the most varied technologies, it aims to enable network communication between people, objects and things with different levels of autonomy, extracting and / or providing services and information among themselves or to other devices through the Internet. The IoT architecture can be treated as a physical, virtual or hybrid system, being able to make use of technologies such as Cloud Computing [2], able to overcome the limitations of computing and storage in intelligent devices, besides providing elastic resources to them [3]. According [3], [4] and [5], due to the need to support mobility, geographical distribution, location recognition and low latency demand for some applications, the Cloud meet with some difficulties.

To overcome these difficulties, Cloud features were brought to the edge of the network [6], [7] and [8], thus forming Fog Computing, or simply Fog, which, as a link between IoT and Cloud, induces the extra functionalities required for specific processing of applications, such as filtering and aggregation, before transferring the data to the Cloud [9].

Taking advantage of IoT's capabilities, a wide range of intelligent solutions and applications for the most diverse areas, such as Smart City and Smart Home, have been proposed and increasingly demanded of it, with forecast growth in equipment usage to 50 billion units by 2022, including sensors and actuators [10]. However, this generation advance has been presented in a highly complex way, which has been demanding and moving researchers from the most varied areas of knowledge, besides the need to create environments for the performance analysis of these studies. Some challenges of Fog are listed by [5] and [11], which consider the importance of identifying appropriate techniques and metrics for efficient resource provisioning and management.

In [12], they states that a large number of links and different interactions between edge nodes in IoT makes it a complex and scalable system; therefore, it is difficult to achieve the dynamic requirements of Quality of Service (QoS). How described in [13] and [11] argue that the absence of Service Level Agreement (SLA) management, as well as sustainable metrics, make it difficult to maintain a QoS acceptable in highly dynamic environments. This increase in the number of devices on the network also creates security-related issues, making these endpoints an easy target for malicious people to compromise these devices for use in large-scale attacks.

Thus, our paper aims to present a Fog Computing architecture to provide QoS and security through an orchestrated and virtualized environment, including characteristics such as interoperability and scalability.

The remainder of this paper is structured as follows: Section 2 describes the Fog Computing architeture applied in this study. Next, section 3 presents the implementation issues, followed by related works in the section 4. Section 5 presents a Conclusion.

II. Fog Computing Architecture

According to the paper presented by [14], six criteria considered important for the Fog Computing architecture are: Heterogeneity, QoS Management, Scalability, Mobility, Federation and Interoperability. The architecture we propose next, not only to meet some of these criteria, as well as aspects related to security, providing a consistent, manageable, and secure environment with characteristics that may facilitate the commercialization of services implemented.

This study was financed in part by the Coordenacao de Aperfeicoamento de Pessoal de Nivel Superior - Brasil (CAPES) - Finance Code 001.

These approaches, when contemplated by other articles, are solved individually or in smaller numbers, as we can observe in topic IV (related works). In addition, we are not aware of the use of the K-means algorithm in a Fog Computing.

The proposal of our paper is based on the use of a three-layer architecture similar to that proposed by [4], concomitantly contemplating the six functional blocks of IoT presented by [2] (devices, comunication, services, management, security and application).

As we can see from the Fig. 1, the architecture presents the layers in a well-defined way, where we have the tradicional Cloud at one end, the Fog at the interim layer (composed by Fog nodes) and the edge with the IoT devices. The IoT devices are one of the aforementioned functional blocks, being sensors, actuators, smartphones, among others capable of generating and consuming Fog data.

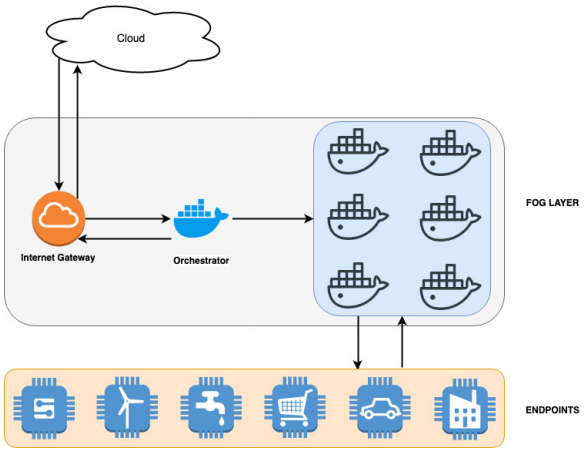

Fig. 1. Fog Archteture proposal.

Interoperability between layers and devices is achieved through the functional block of communication, by means of the data links and their virtualized infrastructure, since much of it is based on Docker containers. Although there are other solutions that promote the use of containers, the Docker offers fault tolerance, service management and deployment capabilities that facilitate the solution delivery process.

Virtualization is a strong trend in the implementation of Fog Computing architectures as we will see in the related works of this paper, making it possible to meet the federation criterion if it becomes a standard used by other service providers, in addition, it makes the architecture scalable through use of a swarm structure, allowing to act in order to deliver the solution continuously orchestrated, attending to the service block.

The last three functional blocks (management, security, and application) are served by another strong feature of this architecture, which is being presented at a time when the threat detection models begin to act directly in Fog layer, allowing the time to decision making is reduced as internal and external threats are identified, thus improving QoS.

This structure will rely on the use of an unsupervised artificial intelligence algorithm capable of learning about anomalies and behavior (DDoS) in a distributed way, which is one of the ten major security flaws in a Fog architecture, according to [15].

As can be seen in the work of [16] and [17], the use of the K-means algorithm presented a very high hit rate compared to other techniques. This algorithm will run in the Cloud (Fig. 2) for training and validation of the samples. Will learn by behavior patterns from open source datasets and then send information to the orchestrator at Fog Computing who will be responsible for generating metrics about the environment as well as resource provisioning computational linked to the models learned in the Cloud.

The orchestrator registers the status of all fog nodes, including the activation and disconnection of nodes, the type of nodes and the IP address of each of them, and is responsible for managing the resources of those nodes that will communicate with the endpoints.

The resources management, among its characteristics, will enable the architecture to simultaneously meet the demands of applications that have or do not have restrictions in real time, prioritizing the guarantee of resources for the most needed or that there is an SLA contract with the client.

The model is combined with the use of SDN (Software Defined Networking) devices since it will be responsible for performing the traffic routing to the endpoints, as well as assisting in the detection, since these data are processed by the Fog node and the cluster, thus providing a better distribution of responsibilities and lower latency among taxpayers. The gateway aims to effect separation and translation between the external and internal networks.

III. Implementation Issues

In order for the environment to achieve the objectives proposed by our architecture, we have a hardware and software structure that will be described as follows:

For anomaly processing solution will be used an Amazon Web Services (AWS) as Cloud Computing Services to find patterns of DDoS attacks. The displayed gateway will be set by a raspberry pi 3 device running the Raspbian Stretch Lite operating system. In order to be orchestrated, 2 physical machines configured with 3.2 Ghz i5 processors and 8 GB ram DDR3 memory will be used, running the linux operating system in the debian 9.9 distribution, as well as the Docker Community edition in version 17.12.1-ce where the portainer management configured, with the portainer/portainer image being available in the Docker hub, chosen for this experiment.

This tool contributes the orchestration of the services in a facilitated way through the use of the webhooks, increasing the practicality in the process of automation of deploy of the final application in the containers that will be destined to solution of SDN.

The area marked in blue in Fig. 2 is responsible for manipulating Fog traffic with IoT devices, applying the rules learned through the cloud and identifying it as malicious or not according to its characteristics. Considering that the entire decision-making process should be automated, this

environment is supported by SDN, responsible for providing the necessary intelligence and automation, creating intelligent routes according to the context.

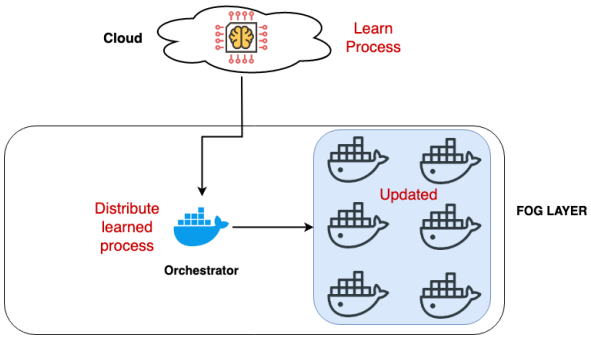

Fig. 2. Fog Security Service.

IV. Related Work

In this session, we discussed the studies considered relevant to our work and commented on the tools, devices, and algorithms most used by them, aiming at a better view of trends and how research in the field of Fog Computing has been developing.

Most of the papers were identified through the systematic mapping process proposed by [18], where we considered the Fog Computing architectures approach that involved both quality of service issues including performance analysis for intelligent environments, as well as questions of security. In this way, we analyze these issues separately in order to facilitate understanding.

A. Related works to architecture in QoS context:

In [19], is present a layered architecture called Fog-to-Cloud (F2C) and compare with an optimized F2C (OF2C) and the traditional Cloud, presenting through simulation and use case in health care the benefits of running services in the different F2C layers. As a result, using the Tareador and Paraver tools, the authors demonstrate an improvement in the task execution speed of 32,05% of the OF2C architecture in relation to the traditional Cloud and poses as a challenge the creation of resource management strategies in different layers of F2C to provide QoS.

A implement through simulation with a framework called Stack4Things, structure based on OpenStack that includes IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) is presented by [20]. They also present a case study of environmental data collection through #SmartME (project to stimulate the creation of a new virtual ecosystem of smart city for the Messina's city). This work indicates anothers types of services that will be provided by Fog, reinforcing the suggestion made by [11] that adapting the Cloud SLA to Fog Computing may be a possible solution for the implementation of this agreement and also as an aid to QoS.

The efficient sharing of client network resources covered by [21], creates network layers configured using SDN and VNF deployed on low-cost common network devices (EX: Raspberry) to approximate wireless and custom services of mobile devices and sensors . As a result, the average cloud delay was approximately 133 ms, versus 12 and 5.3 ms for single board and PC computers, respectively. The environment configured in this work is approximated with the outline of our proposal.

An anomaly detection solution for the smart city application based on Fog, connected to LPWAN and evaluated through algorithms in the testbed of the city of Antwerp is proposed by [22]. The results show that both the Birch cluster and the RC anomaly detection mechanisms can be executed by Fog features. The LPWAN technologies evaluated and validated for the application of air quality were: IEEE 802.11ah, DASH7 and LTE-M.

In [23] study the issue of resource continuity and coordinated Fog and Cloud management and propose the fundamental blocks for system architecture. They demonstrate the benefits of a layer management approach by considering the size and time to search for smart city databases. The authors observed that the smaller the city area the smaller the database size, the lookup time, the lower the number of services to be executed, and thus the lower the interest in these services by the users.

The use of the SDN architecture in a Fog Computing architecture is proposed by [24], focusing on real-time vehicle traffic management, seeking performance enhancement and improved traffic management and QoS in real-time data distribution. In this work, an architecture similar to the one proposed in this paper is used, but its objective is to use it in a vehicular environment.

B. Works related to security issues:

Presented by [25] on his work about Deep Learning on despite the success of traditional Internet cryptographic solutions, factors such as system development flaws, increased attack surfaces, and hacking skills have proven the inevitability of detection mechanisms. Traditional approaches to machine-based attack detection have been successful in the last few decades, but it has already been proven that they have low accuracy and less scalability for detecting cyber attacks on massively distributed nodes such as IoT. The proliferation of deep learning and technological advancement of hardware can pave the way for the detection of the current level of sophistication of cyber attacks in high-end networks. The application of deep networks has already been successful in large areas of data, and this indicates that end-to-end computing may be the ultimate beneficiary of the attack detection approach because a large amount of data produced by IoT devices that deep models learn better than surface algorithms and showed that Deep Learning (DL) models perform well when using unsupervised learning in Zero Day applications, improving model accuracy in invisible and mutant attacks.

In [26] has defined Fog Computing as a new paradigm with many different features of Cloud Computing. Because features are limited, Mobile Edge Computing (MEC) Fog nodes / hosts

are vulnerable to cyber attacks. IDS is a fundamental technique for solving the problem. As the Extreme Learning Machine (ELM) has the characteristics of rapid training speed and good generalization capability, a new light IDS called the extreme selection machine (SS-ELM) is presented. The reason why this new model is proposed is justified because the Fog nodes / MEC hosts do not have the capacity to store extremely large amounts of training data sets. Thus, they are stored, calculated and sampled by the Cloud servers. Then the selected sample is supplied to the Fog / MEC hosts for training. This design can reduce training time and increase detection accuracy. The experimental simulation verifies if the SS-ELM shows good intrusion detection performance in terms of accuracy, training time and receiver operating characteristic (ROC) value.

According to the work of [27] as proposed for IoT applications in which it uses Fog Computing to implement an intrusion detection based on the distributed model. The proposed system consists of two modules: Detection of Fog node attacks and summarization on a Cloud server. In this work the Extreme Learning Machine (ELM) algorithm was used and from it a variant called Online Sequential ELM (OS-ELM) was created to identify the attacks in the inbound traffic of IoT virtual clusters.

In [28] proposed to use the deep learning approach to understand that for the treatment of a large data demand, this algorithm is resilient against metamorphosis attacks with high detection accuracy. In this work it is proposed the use of an LSTM network for detecting distributed cyber attacks in Fog communication for things. The experiments conducted demonstrate the effectiveness and efficiency of deeper models compared to traditional models of machine learning.

As shown in the article of [16], it was proposed a DDoS detection model with K-Means algorithm customization that compared to other works provided a higher rate of detection of anomalies, taking into account factors such as True Positive Rate, False Positive Rate and Recall Rate. In addition, is used the main Open Source Dataset (DARPA, CAIDA, CICIDS), as well as the real-world dataset to proposed benchmark. It forms very high hit rates compared to related jobs.

V. Conclusion

The systematic mapping process used in this paper was extremely important for the direction in the search for the state of the art, resulting in the theoretical basis and the identification of the current conjuncture of Fog computing as a whole reported in this paper through the introduction and related works. This corroborated for a better view of the architectural tendencies, devices and tools used in a Fog environment, such as we also indicate in our work. The virtualization and testbeds, for example, are quite common in the environment in question.

In this paper, we present a Fog Computing architecture capable of providing a consistent, manageable, secure environment with specific characteristics relevant to a Fog and to IoT, such as interoperability, scalability, management, among others. This is due to the fact that we have used a virtualized, orchestrated and intelligent environment, a structure that can facilitate the service delivery process between the existing layers in a secure way. The ability to replicate internal security in an agile way is another important aspect to note.

As future work, this architecture model can be validated through simulations, emulations or even applied in production environments, since in the presented model the SDN was used in the application mode through the software Open vSwitch, however, it is interesting to substitute this model by a professional SDN switch. Taking into consideration that the object of study of our work is Fog and its operation, it was not taken into account the fact of security problems in Cloud Computing, and this issue should be treated in another paper with this focus.

The QoS covered in our work makes it possible the service guarantee, contributing to the business aspect of Fog Computing, which is usually the service level agreement (SLA), negotiated between the service provider and the client, but the commercialization of services involving the Fog still need to be researched.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010. doi: 10.1016/j.comnet.2010.05.010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2010.05.010

[2] P. P. Ray, "A survey on Internet of Things architectures," *Journal of King Saud University - Computer and Information Sciences*, vol. 30, no. 3, pp. 291–319, 2016. doi: 10.1016/j.jksuci.2016.10.003. [Online]. Available: https://doi.org/10.1016/j.jksuci.2016.10.003

[3] S. Yi, C. Li, and Q. Li, "A Survey of Fog Computing," *Proceedings of the 2015 Workshop on Mobile Big Data - Mobidata '15*, no. June 2015, pp. 37–42, 2015. doi: 10.1145/2757384.2757397. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2757384.2757397

[4] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog Computing and Its Role in the Internet of Things," pp. 13–15, 2012.

[5] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog Computing: A Taxonomy, Survey and Future Directions," pp. 1–28, 2016. doi: 10.1007/978-981-10-5861-5_5. [Online]. Available: http://arxiv.org/abs/1611.05539%0Ahttp://dx.doi.org/10.1007/978-981-10-5861-5_5

[6] P. K. Sharma, M. Y. Chen, and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2018. doi: 10.1109/ACCESS.2017.2757955

[7] Y. Ai, M. Peng, and K. Zhang, "Edge computing technologies for Internet of Things: a primer," *Digital Communications and Networks*, vol. 4, no. 2, pp. 77–86, 2018. doi: 10.1016/j.dcan.2017.07.001. [Online]. Available: https://doi.org/10.1016/j.dcan.2017.07.001

[8] K. Vohra and M. Dave, "Multi-Authority Attribute Based Data Access Control in Fog Computing," *Procedia Computer Science*, vol. 132, pp. 1449–1457, 2018. doi: 10.1016/j.procs.2018.05.078. [Online]. Available: https://doi.org/10.1016/j.procs.2018.05.078

[9] F. Al-Doghman, Z. Chaczko, A. R. Ajayan, and R. Klempous, "A review on Fog Computing technology," *2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 001 525–001 530, 2016. doi: 10.1109/SMC.2016.7844455. [Online]. Available: http://ieeexplore.ieee.org/document/7844455/

[10] K. Yasumoto, H. Yamaguchi, and H. Shigeno, "Survey of Real-time Processing Technologies of IoT Data Streams," *Journal of Information Processing*, vol. 24, no. 2, pp. 195–202, 2016. doi: 10.2197/ipsjjip.24.195

[11] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 1, pp. 416–464, 2018. doi: 10.1109/COMST.2017.2771153

[12] L. Li, S. Li, and S. Zhao, "QoS-Aware scheduling of services-oriented internet of things," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1497–1507, 2014. doi: 10.1109/TII.2014.2306782

[13] R. Prodan and S. Ostermann, "A survey and taxonomy of infrastructure as a service and web hosting cloud providers," *Proceedings - IEEE/ACM International Workshop on Grid Computing*, pp. 17–25, 2009. doi: 10.1109/GRID.2009.5353074

[14] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 1, pp. 416–464, 2018. doi: 10.1109/COMST.2017.2771153

[15] A. Aljumah and T. A. Ahanger, "Fog computing and security issues: A review," in *2018 7th International Conference on Computers Communications and Control (ICCCC)*, May 2018. doi: 10.1109/ICCCC.2018.8390464 pp. 237–239.

[16] Y. Gu, K. Li, Z. Guo, and Y. Wang, "Semi-supervised k-means ddos detection method using hybrid feature selection algorithm," *IEEE Access*, vol. PP, pp. 1–1, 05 2019. doi: 10.1109/ACCESS.2019.2917532

[17] M. I. W. Pramana, Y. Purwanto, and F. Y. Suratman, "Ddos detection using modified k-means clustering with chain initialization over landmark window," in *2015 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)*, Aug 2015. doi: 10.1109/ICCEREC.2015.7337056 pp. 7–11.

[18] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic Mapping Studies in Software Engineering," *12Th International Conference on Evaluation and Assessment in Software Engineering*, vol. 17, p. 10, 2008. doi: 10.1142/S0218194007003112. [Online]. Available: http://www.cse.chalmers.se/~feldt/publications/petersen_ease08_sysmap_studies_in_se.pdf

[19] X. Masip-Bruin, E. Marï£¡n-Tordera, G. Tashakor, A. Jukan, and G. Ren, "Foggy clouds and cloudy fogs: a real need for coordinated management of fog-to-cloud computing systems," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 120–128, 2016. doi: 10.1109/MWC.2016.7721750

[20] D. Bruneo, S. Distefano, F. Longo, and G. Merlino, "An IoT Testbed for the Software Defined City Vision: The #SmartMe Project," in *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*, 2016. doi: 10.1109/SMARTCOMP.2016.7501678 pp. 1–6.

[21] M. S. Carmo, S. Jardim, A. V. Neto, R. Aguiar, and D. Corujo, "Towards fog-based slice-defined WLAN infrastructures to cope with future 5G use cases," in *2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)*, 2017. doi: 10.1109/NCA.2017.8171397 pp. 1–5.

[22] J. Santos, P. Leroux, T. Wauters, B. Volckaert, and F. D. Turck, "Anomaly detection for Smart City applications over 5G low power wide area networks," in *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, 2018. doi: 10.1109/NOMS.2018.8406257. ISSN 2374-9709 pp. 1–9.

[23] X. Masip-Bruin, E. Marin-Tordera, A. Jukan, and G.-J. Ren, "Managing resources continuity from the edge to the cloud: Architecture and performance," *Future Generation Computer Systems*, vol. 79, pp. 777–785, 2018. doi: https://doi.org/10.1016/j.future.2017.09.036. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17302686

[24] K. S. Sahoo and B. Sahoo, "SDN Architecture on Fog Devices for Realtime Traffic Management : A Case Study SDN architecture on fog devices for realtime traffic management : A case study," no. October, 2017. doi: 10.1007/978-81-322-3592-7

[25] A. Abeshu and N. Chilamkurti, "Deep Learning: The Frontier for Distributed Attack Detection in Fog-To-Things Computing," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 169–175, 2018. doi: 10.1109/MCOM.2018.1700332

[26] X. An, X. Zhou, X. Lü, F. Lin, and L. Yang, "Sample selected extreme learning machine based intrusion detection in fog computing and MEC," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–10, 2018. doi: 10.1155/2018/7472095

[27] S. Prabavathy, K. Sundarakantham, and S. M. Shalinie, "Design of cognitive fog computing for intrusion detection in Internet of Things," *Journal of Communications and Networks*, vol. 20, no. 3, pp. 291–298, 2018. doi: 10.1109/JCN.2018.000041

[28] A. Diro and N. Chilamkurti, "Leveraging LSTM Networks for Attack Detection in Fog-to-Things Communications," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 124–130, 2018. doi: 10.1109/MCOM.2018.1701270