This is a peer-reviewed, author's accepted manuscript of the following conference paper:
Ugwuanyi, S., Ghanem, K., Hansawangkit, J., McPherson, R., Khan, R., & Irvine, J. (Accepted/In press).
Communication requirements and deployment challenges of cloudlets in smart grid. 1.
Paper presented at 2021 IEEE International Conference on Smart Applications, Communications and Networking, Palapye, Botswana.

Communication Requirements and Deployment Challenges of Cloudlets in Smart Grid

[1]Stephen Ugwuanyi
Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
Stephen.ugwuanyi@strath.ac.uk

[3]Jidapa Hansawangkit
Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
jidapa.hansawangki@strath.ac.uk

[5]Rabia Khan
Power Networks Demonstration Centre
University of Strathclyde
Glasgow, United Kingdom
rabia.khan@strath.ac.uk

[2]Kinan Ghanem
Power Networks Demonstration Centre
University of Strathclyde
Glasgow, United Kingdom
kinan.ghanem@strath.ac.uk

[4]Ross McPherson
Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
ross.mcpherson@strath.ac.uk

[6]James Irvine
Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
j.m.irvine@strath.ac.uk

***Abstract*—Intelligent and distributed power networks are becoming more complex with the addition of cloudlets infrastructure. This paper is the initial output of a Low Latency Edge Containerisation and Virtualisation project at PNDC. This project investigates the performance and communication requirements of deploying edge computing devices to enable low-latency applications. The edge network illustrates how additional intelligent network resources can help realise better-distributed automation and remote configuration in smart grids. With cloudlets, the performance of smart grid networks will be enhanced in terms of low latency, higher bandwidth, and other network requirements. This paper presents cloudlets technology's current state of the art, including network design requirements, implementation techniques, and integration challenges with the legacy power networks. It also explored the main challenges of processing smart grid data by constrained IoT devices. The feasibility of using edge containers to provide low latency communication to several critical end applications in the smart grid could improve the performance of the networks. Furthermore, the key use cases of cloudlets in critical end applications for power utility networks were identified**

Keywords—Cloudlets, Containerisation, Communication Requirements, Deployment, Security, Smart Grid., Virtualisation

I. INTRODUCTION

Overcoming service availability and delay is one of the deployment challenges of the Internet of Things (IoT) technology in power utility networks without centralised cloud infrastructures. Cloud computing, as defined by the National Institute of Standards and Technology (NIST), is a model for facilitating ubiquitous and on-demand access to a shared pool of network resources in three different service models; Software as a Service (SaaS); Platform as a Service (PaaS); and Infrastructure as a Service (IaaS) [1]. While each service model can be provisioned with network characteristics such as broad network access, on-demand self-service, resource pooling, rapid elasticity, and measured service, they could be used in private or public networks or a combination of both. For instance, PaaS resources can be rented to install Supervisory and Data Acquisition System (SCADA) systems to be shared by distributed generation sources and Distributed Network Operators (DNOs) [2].

IoT-based smart grid networks generate massive data from heterogeneous edge devices that require high computing resources to process the data in the cloud and deliver optimal network performance. Strategically placed cloud resources closer to the edge devices will help to offload the massive dynamic traffic generated by the distributed IoT devices to guarantee high quality of services. It will free the smart grid from Wide Area Network (WAN) related delays, jitter, congestion and network failures [3]. Cloud process and compute time required for such high numbers of IoT devices is a bottleneck in today's networks without technology such as cloudlets. It is essential in IoT networks to move data processing points closer to the data sources to meet the communication requirements of real-time applications. It will ensure fast response time and reduce the amount of unnecessary data migrated to the centralised data centre.

Moreover, power utilities avoid using public clouds for critical applications due to latency and security issues. However, they seek an alternative private cloud infrastructure to process the generated data locally and securely before the fine-grained data is sent to the centralised private cloud for other processing that may involve machine learning and artificial intelligence algorithms. This process will provide computing power support for IoT devices when deployed correctly using adequate communication technology such as 5G cellular networks in good coverage [4].

Reducing network response time in mobile utility IoT applications may be challenging as traffic may not be offloaded optimally. To offload traffic optimally requires many factors, like ensuring that cloudlets are optimally positioned with adequate coverage of reliable and bandwidth-efficient communication technology and that the edge devices have enough processing, storage and memory capabilities. An entropy-weight-based proof of concept algorithm found to be optimal, cost-effective and can meet network delay requirements has been proposed to tackle the cloudlets placement problems [5]. Similarly, a dynamic clustering algorithm-based cloudlets deployment is another approach to solving latency issues in cloudlets due to edge device mobility in smart grids [4].

Cloudlets concepts in the smart grid are seen as a data processing approach to moving cloud computing capabilities closer to intelligent field devices and serve limited and localised utility assets like Remote Terminal Units (RTUs) and smart transformers than wider utility IoT resources. As a mini data centre designed to provide cloud computing services to IoT field devices within a close geographical area, it will facilitate edge virtualisation and intelligence. Both enhancements require the proper hardware and software with sufficient processing, memory and real-time operating capability to enable accurate grid data synchronisation for controlled functions, efficiency and the effectiveness of the

978-1-6654-8758-0/22/$31.00 ©2022 IEEE

end applications. Reducing variable latency largely between integrated grid assets benefits utility networks' operation. Cloud infrastructure could be either on-premise or off-premises, but both play essential roles in seamlessly integrating utility assets for easy computation of smart grid data. Cloudlets are the intermediate layers between the cloud infrastructure and utility assets [6]. Introducing a data centre closer to the edge devices would facilitate the virtualisation of substation devices such that edge devices can easily instantiate Virtual Machine (VM) software on the cloudlets.

II. Related Work

Cloud computing is on-demand storage, data processing and information exchange model for enabling global and continuous access to network resource management systems. In [7], it is seen as a trusted cluster of computers connected to the Internet and designed to deliver cloud computing services to IoT devices within a specific geographical neighbourhood. Cloud computing is one solution to reducing resource-constrained IoT devices' impacts on network performance. This can be achieved via VMs, as each connecting user or end application is associated with VM instances created within cloudlets.

In smart grid ecosystems, cloudlet is an evolving cloud computing infrastructure used to federate the associated processing of networking logics embedded in the edge and wireless cloud [2], [8]. Its performance is mainly affected by communication and processing factors. Cloudlet performance in a rural area has been investigated and likened to locations of utility assets. In this study [9], cloudlet is noted to reduce the lack of communication infrastructure barrier in hard-to-reach locations and make power networks more open, inexpensive, adaptable, and an extensible platform only when implemented with higher compute devices. Cloudlets have been deployed in many sectors, including the smart grid [2]. Cloudlet has been used to reduce the execution end time of workflow applications in metropolitan area networks [10]. Well-deployed cloudlets in the secondary or primary substations will reduce the substation-to-substation communication latency between substation devices in Figure 1. The intermediate mini cloud data centre will ensure efficient and secure communication between the grid entities. As shown in Figure **1**, a resource-rich cloudlet will act as an intermediates layer between the cloud resources and utility assets to deliver time-critical applications with minimal hop path and bandwidth. However, cloudlets have key deployment challenges that must be tackled. These challenges will include questions about how smart grid communication protocols could support virtualisation and integrate with new and existing network resources. It will also involve identifying locations for cloudlets placement with adequate network coverage, compatibility, interoperability, scalability, trust, and security.

Notwithstanding that the use of cloudlets in the industry is continuing to grow especially for achieving low latency communication and reducing costs, there are still open research questions on using cloudlets in smart grids. Studies on cloudlets' performance in real smart grid networks are limited. Navantia industrial AR (IAR) network architecture is designed to leverage cloud, cloudlets and fog computing to deliver traffic-efficient industrial IoT networks [11]. The findings indicate that cloudlet's response rate outperformed cloud and fog computing at payloads greater than 128 KB. While this value is four times greater than fog computing when many applications were served, fog computing achieved the fastest response rate for small payloads. Both the cloud and fog computing technologies are ideal for supporting distributed, low-latency and Quality of Service (QoS) aware applications that decrease network latency response.

Similarly, in a cloudlets-based Wireless Local Area Network (WLAN), offloading the MAC layer processing from the access points to the cloudlets allowed flexibility in service provisioning at reduced costs [12]. The capital and operational costs of running a cloudlets-based network in a smart grid will reduce as the network operators could easily implement new services without procuring more expensive equipment. Network Function Virtualisation (NFV) is another aspect of cloudlets that will simplify network management and remote service provisioning, reduce access latency, and make deployment easier to implement.

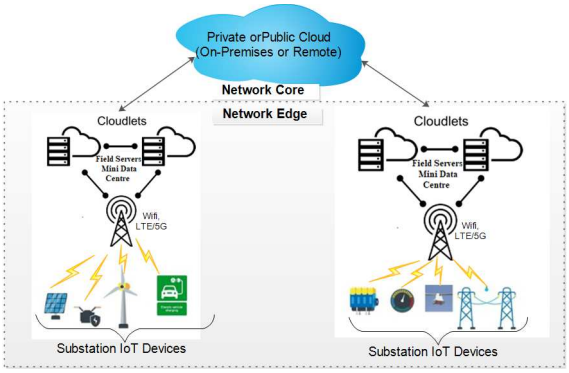

Figure 1. Proposed Cloudlets Supported Smart Grid to Reduced Substation-to-Substation Latency

Figure 1 shows a three-level smart grid infrastructure with integrated IoT systems. The IoT devices provide the field measurements transmitted to the cloud centre for processing through the gateway. In the smart grid, collecting field data measurement, communicating, monitoring, and controlling the distrusted end devices are part of the IoT system's objectives. Field data are better processed in the cloudlets with adequate resources because IoT devices have the lowest computing, storage, and power capabilities to support connectivity solutions for data delivery and analysis. These limitations are responsible for technologies that drive data processing towards the edge to reduce communication latency, especially for time-critical applications. Cloudlets reduce network latency as a localised cloud/data processing point. The unique nature of the power network as an Operational Technology (OT) infrastructure means that connectivity solutions for data transmission between smart grid IoT devices and the cloud centre are not straightforward solutions. It will require open communication frameworks such as OpenFMB for network integration. Hence, deploying cloudlets in the smart grid will allow DNOs to have more network control and quickly provision service functions such as security and privacy.

Cloudlets also need to be coordinated during design and implementation. Coordinated cloudlets are described as small clouds in network infrastructures that are interconnected [13], and each server is discoverable, localised and stateless with one or more VM in operation. An end-to-end direct connection through a Software-Defined Wide Area Network (SD-WAN) could facilitate real-time applications for geographically distributed cloudlets. Installing a cloudlet closer to the IoT field devices will open the door for complete local processing and reduces the time to migrate data to the central cloud or data centre. The cloudlet will be able to host virtual access points, which will also avoid the complexity of a physical access point common in legacy networks [12].

III. IMPLEMENTATION ARCHITECTURE

As shown in Figure 2, the proposed implementation architecture is a new test setup regime at PNDC in collaboration with DNOs for investing cloudlet's performance in smart grids. The RTDS Simulator generates IEC 61850 GOOSE and Active Network Management (ANM) packets, whereas SCADA Simulator generates Modbus and DNP3 used to investigate IT/OT convergence edge container that converts field protocols to OPC/UA. Both simulators exchange data with external hardware or software devices in real time through many different communication protocols. Input and output via Ethernet (though standard-compliant data packets) allow the closed-loop testing of digital substations and other non-wires alternatives. The edge container (cloudlet) has virtualisation and real-time operating system capabilities to process IEC 61850, NDP3, and Modbus protocols while communicating with the ANM system. The development stage of the test platform is shown in Figure 2, along with the design requirements needed to develop the IEC 61850 protocol adaptor in the OT/IT convergence testbed.

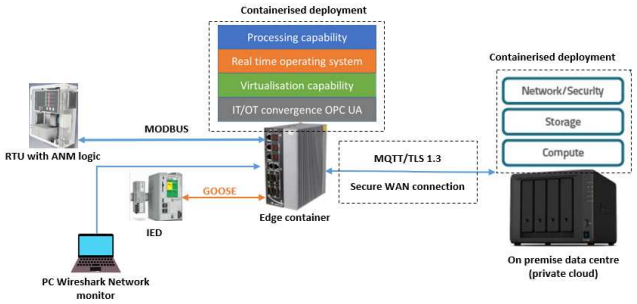

Figure 2. High-Level Cloudnet Test Network Architecture to Facilitate IT/OT Convergence at PNDC.

IV. CLOUDLETS REQUIREMENTS IN SMART GRID

Power networks consist of generation, transmission, and distribution subsystems that deliver electricity to consumers. Its implementation requires dedicated, secure and reliable technologies for monitoring, communicating and controlling grid assets in a two-way fashion. Cloudlets could help deliver security [14] - [15], computing [7], communication [16], and data storage network requirements in smart grids. Some of these performance specifications are better defined by the DNOs, regulators, policy-makers and vendors. They include:

A. Communication Technology

Connectivity for cloudlets-based critical applications such as teleprotection requires very low latency delivered by LTE or 5G networks to maintain data synchronisation among multiple devices and systems [17]. The frequent exchange of Phasor Measurement Unit (PMU) data and control commands between substations and the control centre requires a robust, reliable, low-latency communication link across the network. The same communication requirements are needed for critical IEC 61850 Sample Values (SV) and GOOSE messages. Cloudlets could be seen as a proper technique for providing low-latency communication if the field measurement data are processed at the network edge [18]. For some critical applications, the required end-to-end latency to enable the functionality of PMU synchrophasor is 100 ms and around 1 ms for critical control commands, which can be challenging to satisfy.

B. Resilience and Redundancy

In the smart grid, fibre optics, LTE, and 5G will play an important role in completing the path to full digitalisation of power networks. Critical end applications such as synchrophasor data and any routable GOOSE messages will require redundancy to ensure resilience in case of any problem in the connection to the data centre or with another cloudlet. As fully identified in the meshed cloudlets in Figure **5**, smart grid resources must be integrated with robust, reliable, low latency communication technology. With cloudlets, smart grid assets must support network virtualisation technologies such as Network Function Virtualisation (NFV) and Software Defined Network (SDN) to simplify such complex and meshed networks.

C. Privacy and Security

Cloudlets may face privacy and security requirements in smart grids, especially when data is distributed and shared across multiple entities with less computational and storage capabilities. When moving the processing capabilities to the edge, the security approach used at the main data centre could be applied in the cloudlets. Implementing end-to-end encryption at the edge without compromising security and privacy has always been challenging. In [14], a TLS-based secure protocol extension proposed could allow edge functions to process encrypted traffic at the edge of an IoT network. However, our previous study identified that implementing encryption techniques such as TLS and IPsec within the utility assets will increase the data overhead by a significant fold [19]. Encrypting the exchanged data among different systems and devices using strong encryption keys will raise an issue about the bandwidth requirements needed to enable low latency communication [20]. Cloudlets in the OT environment could become challenging to manage from a security perspective. Smart grid networks could be made less secure due to the limited number of Information Technology (IT) security layers and its interoperability issues with the OT security layers in resource-constrained devices. Because cloudlets are more accessible and interfaced with less secure IoT devices, their use in smart grids will require more protection to secure the local data storage systems and the communication link between the cloud, cloudlets and the field devices.

Ensuring that cloudlets technology satisfies cyber security standards like NIST/ENA/IEC guidelines and policies, including supporting utility protocols such as Modbus, DNP3, IEC 60870-5-104, 60870-5-101 and IEC61850 securely, reliably and at low costs are essential. Smart grid communication protocols carry a large amount of sensitive time-critical utility data prone to intrusion, subversion, or spoofing attacks. Because cloudlets have the capability to create meshed networks with a shared medium of high availability when deployed in smart grids, their vulnerabilities, threats, and impacts need to be risk assessed.

D. Storage

Smart grid network resources like PMUs and Intelligent Electronic Devices (IEDs) generate crucial time-sensitive data requiring appropriate data storage systems. According to the Utility AMI Working Group, utility data storage systems must be long-term and able to store data within the device securely. In the case of a smart meter, the data must be stored for 45 days [21]. The data must be accessible remotely and with a standard model that allows it to be exchanged between multiple vendors' equipment. The rise of the Smart Storage

(SS) systems, Distributed Energy Resources (DERs), and Electric Vehicles (EVs) will increase the need for efficient and reliable storage systems. Cloudlets will enable fast implementation of Virtual Power Plant (VPP) and microgrids for controlling the DERs. It will also help DNOs identify and locate DERs for energy usage measurements and analysis.

E. Disaster Recovery

Cloudlets introduce redundancy to the power networks as critical processing at the edge can be continued through cloudlets when the main cloud infrastructure fails [18]. The capability of the smart grid to function as a standalone in disaster and blackout scenarios is essential to enable basic functions like communicating with the secondary data centre when required. However, cloudlets functionalities may be lost in natural disasters, including processing, storage and power sources. Cloudlet outage must be avoided as critical services could be interrupted, frozen and QoS violated.

To analyse the impact of these network characteristics on smart grid performance, we have discussed three different scenarios in which cloudlets architecture could be configured. The first is a multi-access cloudlets architecture shown in Figure **3**. Multi-access cloudlets enable the integration of several smart grid assets and deliver services and computing functions needed by the end applications. With the massive amount of devices at the edge and high variation of data-intensive applications, 5G/6G networks have been noted to meet such demands in the future cloud and communications networks [22]. This will improve application response, enhance outage control, and support new applications in smart grids.

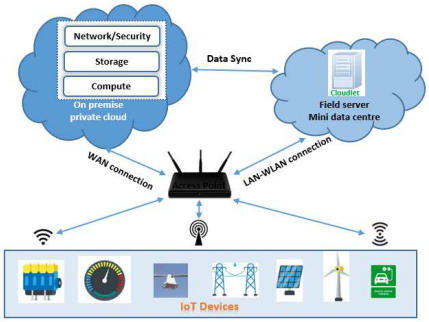

Figure 3. Multi-Access Cloudlets Architecture

In this paper, we see cloudlets deployment in power networks as a standalone edge processing box within the secondary or primary substations with sufficient power backup, where direct connectivity is provided to restore service outages. As shown in Figure **4**, connectivity to the private cloud infrastructure is not always needed to provide the required services, and data synchronisation with the private cloud could be initiated when cloud connectivity becomes available.

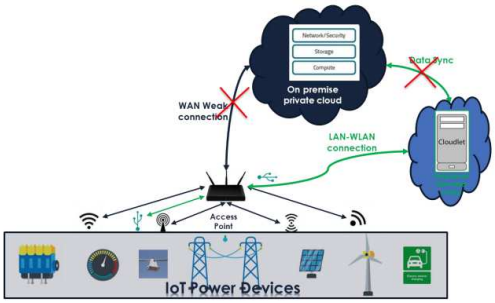

Figure 4. High-Level Standalone Cloudlet Topology at the Edge.

While the best deployment option that could be expected of a cloudlet's architecture in a smart grid is a fully meshed network, as shown in Figure **5**, it must be designed following the European Telecommunication Standards Institute (ETSI) Multi-Access Edge Computing (MEC) standard [22]. The operation of fully meshed cloudlets in power networks requires a private network fully operational and managed by the power utilities. Accurate data synchronisation and the number of hops between cloudlets and IoT field devices, connectivity and security are a few challenges that might be seen in a fully meshed scenario.

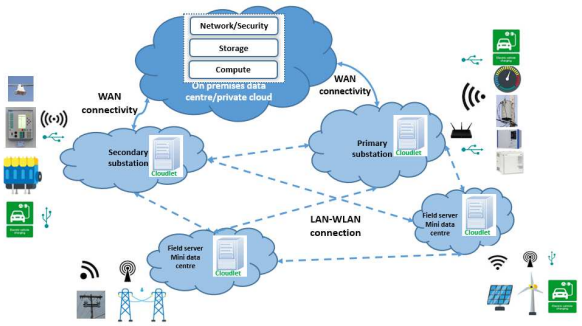

Figure 5. Fully Meshed Multi-Access Cloudlet Architecture

V. CLOUDLETS CHALLENGES IN POWER NETWORKS

Significant benefits can be obtained by deploying cloudlets in critical infrastructures such as power networks, as they can give the DNOs full control over their distributed infrastructure in terms of implementation, management and security. However, its deployment faces the following challenges:

A. Lack of Skilled Professionals

Cloudlet is a cloud computing technology which can deliver hosted services to IoT devices over a network. It is advantageous to deploy cloudlets on the power network's edge compared to the public cloud, where the enterprise cloud operators manage it. With cloudlet technology at the edge of power networks, DNOs can easily deploy and manage their infrastructure if adequate skilled network professionals are available. The lack of skilled professionals is challenging to many existing DNOs, and relying on a third party to operate the cloudlet may not apply to some DNOs for security and privacy reasons. Notwithstanding, skilled IT professionals will be needed to define the most appropriate cloudlet technology and its operational requirements in power networks. Recent developments are expanding the use of OpenFMB and OpenADR to meet the needs of utilities, but their implementation requires skilled professionals.

B. Communication Frameworks Integration

One challenge facing utility operators is communicating with more distributed energy resources (PVs, batteries, EVs, etc.) without improving the network architecture. Open Field Message Bus (OpenFMB) and Open Automated Demand Response Communications Specification (OpenADR) are two widely used open communication frameworks in smart grids for network integration [23]. OpenFMB is a framework that functions with new and existing standards, such as the IEC 61968 for distributed edge intelligence designed to drive interoperability and facilitate data exchange between field devices. It has an agile and evolving architecture that is flexible enough to handle data models and publish/subscribe protocols like MQTT and AMQP. OpenADR is designed to

facilitate automated Demand Response (DR) actions at the customer location, using load shedding or shifting. It provides continuous dynamic price signals such as hourly day-ahead or day-of real-time pricing. Today, utilities worldwide are investigating OpenADR to manage the growing demand for electricity and the peak capacity of electric systems. Demand-side resource aggregation by Pearlstone Energy and National grid [24] and Project ELBE [25] are good examples.

C. Data Synchronisation Challenges

Smart grid networks use precision timing of grid assets' information to manage and maintain the operation of the power network. Connecting IEDs to a cloudlet requires precise synchronisation of various data types and several sources of measurement. Synchronising data measurements is crucial for critical end applications such as synchrophasors and protection systems. The required synchronisation accuracy varies based on the criticality of the end applications. Achieving local synchronisation is easier than remote synchronisation, as it is easier to coordinate precisely with other systems' components in real time with fewer errors and duplications.

Moreover, ensuring synchronisation among multiple cloudlets is significant for any future development of the cloudlets in the power networks. Losing such synchronisation limits cloudlet usage in power networks and creates a less efficient power network management system that performs below expectations. Measurements such as outputs from synchrophasors (Sampled Values (SV) and GOOSE) are synchronised with precise timing stamps. Deviations from the synchronisation could create disruption and instability in the power networks. In today's networks, DNOs need accurate time synchronisation in phasor measurement units, merging units and IEDs to coordinate the electrical grid and monitor protection functions. Deploying cloudlets in smart grids requires precise time synchronisation to utilise the cloudlet capability fully.

D. Systems Integration and Legacy Challenge

Legacy systems in power networks may not directly communicate with new utility IoT devices without protocol conversions. These devices could create several issues affecting the power grid's digitalisation. Legacy hardware is seen as a severe bottleneck to enhancing the future operating capacity of power networks. Upgrading such field devices may not be the right solution for digitalisation, where some old devices may not be upgradeable. Assuming that some of the distributed assets can be upgraded, the time and cost of procuring and installing new devices will be saved. Systems integration is another challenge for DNOs to overcome during the digital transition period. Dealing with too many different protocols and the lack of interoperability will add more complexity to the network architecture that the DNO's whole system could affect cloudlets integration and field implementations.

E. Connectivity and Power

A significant part of the distributed power networks is located in hard-to-reach areas where affording simple connectivity can be challenging. Lack of connectivity does not just limit the ability to deploy cloudlet but also slows the transition into a smarter digital grid. This is a common issue for many power utilities across the world. Another point to consider is that there is no processing and connectivity without power. The lack of backup power will delay the recovery of any power cuts, power outages and blackouts. Ensuring a sufficient source of backup power (i.e., from battery storage for instant or renewable energy sources) will allow the power networks to rely on the communication network to bring the electricity back in case of an unexpected power loss or black start scenario. Full backup power will be required to enable the full functionality of cloudlets. Reliable backup power for distributed cloudlets is a must to maintain any mission-critical applications.

A real concern in the existing power networks is the proprietary interfaces and protocols operated by legacy software. This will significantly affect any future deployment of intelligence at the edge. Converting several field protocols into a unified platform transparent to cloudlet can be seen as a tool to mitigate such challenges. However, there is a need to check the power system performance in terms of data handling and data polling mechanisms.

F. Security

Security and the trust environment used for data storage is a prime issue for cloudlets integration in smart grid. This is because compromised cloudlets cannot attain the mission-critical requirements of power networks. An example of a physical security challenge is protecting a cluster of digital substations connected using cloudlets, where they could share and exchange data locally without involving the centralised data centre. Data storage in the distributed local cloudlets could make them vulnerable to physical attack, as the location of some cloudlet boxes in the rural areas will make it easier for physical access. Cloudlet's physical proximity to the edge is also very essential to achieving end-to-end response time, low-latency, one-hop, high bandwidth wireless access to the cloud [7]. Physical security is a less explored area in cloudlets, according to a study that investigated cloudlets deployment options in rural and remote areas to improve service availability and support community-based local services during network or power outages [9]. Collaboration Intrusion and Detection System proposed for incorporating security, data sharing, and interruption discovery in cloudlets to protect network privacy and the distribution of cloud and cloud medical applications could offer the needed security for smart grid [15].

To deploy cloudlets in the smart grid, security is one factor of high interest to the DNOs. The requirement is that cloudlets have to be remotely managed and provisioned adequately to enhance security and performance [13]. As new security measures can be provided on-demand and customisable through NFV, security functions like next-generation firewalls, gateways, and access policies could easily be implemented. A good example is the proof of concept described in [26] that would allow device-to-device and device-to-infrastructure communication in a cloudlets-supported network and can ensure the reliability, security and privacy of peer-to-peer communication in an intelligent transportation system.

VI. Benefits of Deploying Cloudlets in Power Networks

As an emerging technology, the use of cloudlets in smart grids is accelerating daily and has several benefits, such as rapid response, disaster recovery, outage control, and new technologies [18]. The edge devices and the centralised cloud introduce intelligence to support new utility technology. This

gives the DNOs complete control over their infrastructure in terms of network implementation, resource management, and security. It can also open the door for more real-time applications at the edge, where low latency distributed functions and applications are needed.

Cloudlets technology benefits various sections of the power network. In the primary substations, the data generated from the distributed IoT devices (i.e., distributed IEDs such as Merging Units (MUs) and protections relays) could be processed locally, thereby helping to meet the strict latency requirements for different real-time applications and at the same time ensure that the generated data are kept on-premise securely. It could also facilitate using real-time applications such as Virtual Reality (VR), Augmented Reality (AR), and live machine learning models at the edge. The cloudlets at the primary substation should have more processing capabilities than those installed at the secondary substation because the required processing capability is higher at the primary substation level rather than at the secondary substation level. This will allow sychrophasors, SV and GOOSE messages to be processed quicker than MMS and SCADA messages generated at the secondary substation level.

Another key benefit for energy utilities from implementing cloudlets in smart grids is horizontal and vertical network extendibility. Cloudlets allow the smart grid utilities to timely respond to distribution, generation, market or regulatory changes across various services. Implementing cloudlets with rich computational capability will help deploy several security approaches and techniques between the cloudlet and the end devices as larger key sizes will be supported.

VII. Possible Future Research

The next phase of this low latency edge container and virtualisation project at PNDC will be testing and data analysis to demonstrate how such intelligence at the edge could help improve the performance of the power networks communications in terms of latency and bandwidth to ensure the reliability and resilience of smart grid networks. The cost implications of deploying cloudlets in a secondary substation will also be considered.

IX. Conclusion

This paper has evaluated how the intelligence at the edge of a smart grid can help achieve network performance improvements in distributed automation and remote configuration of smart grid assets. We, therefore, conclude that deploying cloudlets in a smart grid comes with challenges such as systems integration, connectivity, security and the absence of standards-based field bus protocol to enable the interoperability of distributed field devices and data exchange. The challenges are summarised as service description, management and orchestration, monitoring and optimisation, VM placement, and elasticity and scalability-related problems similar to challenges identified in [12]. With the possibility of implementing OpenFMB and OpenADR standards inside the cloudlets, devices from different vendors and utilities will be able to interoperate directly and exchange data. Additionally, if configured correctly, the cloudlets will process data locally and respond to any field requests, facilitating remote-oriented functions that are very useful in an unexpected event or black start scenario.

Acknowledgment

The authors acknowledge the contributions of PNDC tier 1 members (mainly - Scottish Power Energy Networks, Scottish and Southern Electricity Networks, UK Power Networks, Vodafone, and Virtual Access) for funding and supporting this research project.

References

[1] P. Mell and T. Grance, “The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology,” 2011.

[2] M. Muzakkir Hussain, M. Saad Alam, and M. M. Sufyan Beg, “Fog Computing for Smart Grid Transition: Requirements, Prospects, Status Quos, and Challenges,” *EAI/Springer Innov. Commun. Comput.*, pp. 47–61, 2021.

[3] S. Bouzefrane, A. F. B. Mostefa, F. Houacine, and H. Cagnon, “Cloudlets authentication in nfc-based mobile computing,” *Proc. - 2nd IEEE Int. Conf. Mob. Cloud Comput. Serv. Eng. MobileCloud 2014*, pp. 267–272, 2014.

[4] X. Jin, F. Gao, Z. Wang, and Y. Chen, “Optimal deployment of mobile cloudlets for mobile applications in edge computing,” *J. Supercomput.*, vol. 78, no. 6, pp. 7888–7907, Apr. 2022.

[5] C. Guo *et al.*, “Optimal Placement of Cloudlets Considering Electric Power Communication Network and Renewable Energy Resource,” *Proc. - 4th IEEE Int. Conf. Smart Cloud, SmartCloud 2019 3rd Int. Symp. Reinf. Learn. ISRL 2019*, pp. 199–203, Dec. 2019.

[6] I. Stojmenovic, “Fog computing: A cloud to the ground support for smart things and machine-to-machine networks,” *2014 Australas. Telecommun. Networks Appl. Conf. ATNAC 2014*, pp. 117–122, Jan. 2015.

[7] M. Satyanarayanan, P. Bahl, R. Cáceres, and N. Davies, “The case for VM-based cloudlets in mobile computing,” *IEEE Pervasive Comput.*, vol. 8, no. 4, pp. 14–23, Oct. 2009.

[8] S. Mehmi, H. K. Verma, and A. L. Sangal, “Comparative Analysis of Cloudlet Completion Time in Time and Space Shared Allocation Policies During Attack on Smart Grid Cloud,” *Procedia Comput. Sci.*, vol. 94, pp. 435–440, Jan. 2016.

[9] S. Helmer Claus Pahl Julian Sanin Lorenzo Miori Stefan Brocanelli Filippo Cardano Daniele Gadler Daniel Morandini Alessandro Piccoli Saifur Salam Alam Mahabub Sharear Angelo Ventura, P. Abrahamsson, and T. Daniel Oyetoyan, “Bringing the Cloud to Rural and Remote Areas via Cloudlets,” 2016.

[10] X. Zhao, C. Lin, and J. Zhang, “Cloudlet deployment for workflow applications in a mobile edge computing-wireless metropolitan area network,” *Peer-to-Peer Netw. Appl.*, vol. 15, no. 1, pp. 739–750, Jan. 2022.

[11] T. M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela, and M. Vilar-Montesinos, “A Fog Computing and Cloudlet Based Augmented Reality System for the Industry 4.0 Shipyard,” 2018.

[12] F. Ben Jemaa, G. Pujolle, and M. Pariente, “Cloudlet- and NFV-based carrier Wi-Fi architecture for a wider range of services,” *Ann. des Telecommun. Telecommun.*, vol. 71, no. 11–12, pp. 617–624, Dec. 2016.

[13] A. Alsaleh, “Can cloudlet coordination support cloud computing infrastructure?,” *J. Cloud Comput.*, vol. 7, no. 1, pp. 1–12, Dec. 2018.

[14] K. Bhardwaj, M.-W. Shih, A. Gavrilovska, T. Kim, and C. Song, “SPX: Preserving End-to-End Security for Edge Computing,” Sep. 2018.

[15] M. P. Reddy, A. M. F. Anwar, A. Sahithi, and A. K. Shravani, “Data Security and Vulnerability Prevention for Cloudlet-Based Medical Data Sharing,” *Proc. 5th Int. Conf. Electron. Commun. Aerosp. Technol. ICECA 2021*, pp. 1477–1481, 2021.

[16] M. Rihan and M. Rihan, “Applications and Requirements of Smart Grid,” pp. 47–79, 2019.

[17] K. Ghanem, S. Ugwuanyi, R. Asif, and J. Irvine, “Challenges and Promises of 5G for Smart Grid Teleprotection Applications,” *2021 Int. Symp. Networks, Comput. Commun. ISNCC 2021*, 2021.

[18] M. Babar, M. S. Khan, F. Ali, M. Imran, and M. Shoaib, “Cloudlet Computing: Recent Advances, Taxonomy, and Challenges,” *IEEE Access*, vol. 9, pp. 29609–29622, 2021.

[19] K. Ghanem, J. Hansawangkit, R. Asif, S. Ugwuanyi, R. McPherson, and J. Irvine, “Bandwidth efficient secure authentication and encryption techniques on IEC-60870-5-104 for remote outstations,” *2021 Int. Conf. Smart Appl. Commun. Networking, SmartNets 2021*, Sep. 2021.

[20] K. Ghanem, R. Asif, S. Ugwuanyi, and J. Irvine, “Bandwidth and security requirements for smart grid,” in *IEEE PES Innovative Smart Grid Technologies Conference Europe*, 2020, vol. 2020-Octob.

[21] T. Sato *et al.*, “Smart Grid Standards: Specifications, Requirements, and Technologies,” *Smart Grid Stand. Specif. Requir. Technol.*, pp. 1–463, Feb. 2015.

[22] T. Koketsurodrigues, J. Liu, and N. Kato, “Offloading Decision for Mobile Multi-Access Edge Computing in a Multi-Tiered 6G Network,” *IEEE Trans. Emerg. Top. Comput.*, 2021.

[23] S. Laval, “Duke Energy Emerging Technology Office Open Field Message Bus (OpenFMB): Enabling Distributed Intelligence,” 2019.

[24] OpenADR, “Demand-Side Resource Aggregation.” 2020.

[25] H. Energie and S. Hamburg, “OPENADR EUROPEAN CASE STUDY PROJECT ELBE.” 2020.

[26] M. Gupta, J. Benson, F. Patwa, and R. Sandhu, “Secure V2V and V2I Communication in Intelligent Transportation using Cloudlets,” *IEEE Trans. Serv. Comput.*, pp. 1–1, Sep. 2020.