EAI Endorsed Transactions
on Energy Web
Research Article EAI.EU

Construction and Research on Cloud-edge Collaborative Power Measurement and Security Model

Jiajia Huang [1], Ying Sun [2], Xiao Jiang [3], Youpeng Huang [4], DongXu Zhou[5*]

[1] Guangdong Power Grid Co., Ltd. ShaoGuan Power Supply Bureau. No. 66 Gongye West Road, Wujiang District, Shaoguan City, Guangdong Province, 512000, China

[2] Guangdong Power Grid Corporation No. 757 Dongfeng East Road, Yuexiu District, Guangzhou City, Guangdong Province, 510600, China

[3,4,5] Metrology Center of Guangdong Power Grid Corporation, Yuedian Building No. 8 Shuijungang, Dongfeng East Road, Yuexiu District, Guangzhou City, 510000, China

Abstract

Accurate power consumption assessment is of critical importance in the fast-evolving world of cloud and edge computing. These technologies enable rapid data processing and storage but they also require huge amounts of energy. This energy requirement directly impacts operational costs, as well as environmental responsibility. We are conducting research to develop a specialized cloud-edge power measurement and security model. This model delivers reliable power usage data from these systems while maintaining security for the data they process and store. A combination of simulation-based analysis and real-world experimentation helped us to deliver these results. Monte Carlo based simulations produced power usage predictions under various conditions and Load Testing validated their real-world performance. A Threat Modeling-based security study identified potential vulnerabilities and suggested protection protocols. A collaborative approach enhances power measurements accuracy and encourages secure operation of the combined cloud-edge systems. By fusing these metrics, a more efficient and secure operation of computing resources becomes possible. This research underscores the critical importance of developing advanced techniques for power metering and security in cloud-edge computing systems. Future research may focus on both expanding the model's use to an array of larger, more complex networks, as well as the inclusion of AI driven predictive analytics to amplify accuracy of power management.

Received on 29 September 2023; accepted on 20 March 2024; published on 22 March 2024

Keywords: Cloud-Edge Computing, Power Measurement, Security Model, Collaborative Systems, Smart Grids.

doi:10.4108/ew.5522

*Corresponding author. Email: zhoudongxu_jlzx@163.com

1. Introduction

Cloud and edge computing are pivotal to the evolution of power systems in the digital age, transforming the processing, storage, and access of data. These technologies feature remarkable versatility and efficiency, but they are riddled with challenges, particularly regarding power metering and security. The growing adoption of cloud and edge computing infrastructures demands novel power management solutions in order to ensure continued operational sustainability and reduce their environmental footprint. The distributed nature of these systems presents a slew of security vulnerabilities that must be addressed to protect the sensitive data within them [1].

New power metering strategies are needed for cloud and edge computing. They cannot rely on the continuous and omnipresent computer architecture of classic power management. Strong security is needed for the systems that are handling more sensitive and mission critical data. This intersection of power measurement and system security is an area rich with study and development. In this research study we are developing and testing a cloud-edge collaborative

security and power metering architecture. This device will provide high-fidelity and real-time power consumption data and advanced security to thwart the latest threats. Both will improve cloud and edge computing efficiency and resiliency. The test uses Monte Carlo to simulate power state because it can model complex systems and predict outcomes that are not certain. We can test how peak loads and idle intervals may be used by these computer systems [3]. Load Testing is used to stress test the model with real-world conditions in addition to the simulations, where the system is put to the test in varying demand to see power draw and response times, to ensure that the model's predictions match with real life operational data, keeping the model relevant and applicable to a real world setting.

For security analysis in this research, we are deploying Threat Modeling where potential vulnerabilities are discovered and the risks and impacts of different security threats are assessed, these vulnerabilities, in their case the cloud-edge system are viewed from an attacker's perspective, and powerful counter measures can be developed and evaluated, drastically improving the posture of the system [4]. Results showed that the collaborative paradigm delivers fast, accurate power measurements for the real world load measurements and offers strong security in terms of securing deployments. The simulation and real world load tests validate that the model can accurately predict the trend of power consumption, enabling more efficient resource management while the security analysis shows that potential threats can be detected and rolled up. This research holds broad implications the collaborative model sets a new bar in operational efficiency and security for the cloud and edge, representing a way of delivering accurate and prompt power measurements with strong security safeguards. This could yield savings in the cloud space, potentially leading to reduced environmental footprint from the cloud and build further confidence in trusting cloud and edge computing. The advancement of cloud and edge computing calls for innovative strategies that handle the associated power management and security hardships. The collaborative paradigm in this study represents a notable step, bundling meticulous power monitoring with rigorous security protocols. The blend of simulation-based analysis, real-world experimentation and comprehensive security evaluation give a strong foundation for establishing and testing the model. The work is rare in that respect, and it's crucial to guarantee that cloud and edge computing technology can really satisfy the efficiency, sustainability and security needs in the rapidly changing digital landscape. Future projects in the field could expand the model to larger, more intricate networks, and may involve integrating AI to boost predictive capabilities and thus forge ahead in power management and security for cloud-edge scenarios [5].

2. Literature Review

Cloud and edge computing technologies have revolutionized the management and operation of power systems. Consequently, these infrastructures have received increased attention in recent years, with a growing body of research focused on enhancing the power efficiency and security of these systems, as revealed in this literature review. Cloud computing originally emerged in the 1960s with the introduction of time-sharing and the advancement of the virtual machine. Since the early 2000s, cloud computing has provided scalable and elastic compute resources over the internet. More recently, edge computing, which processes data locally, has reduced latency and bandwidth. Real-time analysis, decentralized control, and applications in the world of edge computing have revolutionized power system data management [1]. Earlier research into cloud and edge computing focused on computational operations and data storage. However, as these computing technologies became critical for power system operations, energy efficiency and security gained importance [2]. Power metering must be accurate for cloud and edge architectures to be operationally efficient and sustainable. Direct metering and model-based estimation are two power measurement methods tailored to these contexts. Direct metering uses physical sensors to measure the consumption of computing power. Using this technique, individuals obtain accurate results, but it's expensive and invasive, especially in cloud data centers, where there are so many collocated resources [7].

Model-based estimation, which uses workload and system performance data and mathematical models to predict power consumption, is less invasive and is scalable to diverse situations, but its accuracy is closely bound to how well the model fits real-world power dynamics. Dynamic Voltage and Frequency Scaling (DVFS) techniques have been used in cloud and edge computing to change power consumption on-the-fly based on workload [9]. There are ongoing challenges with current approaches, which struggle to balance accuracy, scalability, and non-intrusive assessment of power usage in the rapidly changing contexts of cloud and edge computing. Security in cloud and edge computing is multifaceted, comprising data confidentiality, integrity, and availability. Among the many risks associated with these technologies are the distributed characteristics of the technologies themselves, which lead to a multitude of additional security considerations, such as increased attack surface and potential interception of data during transit [8]. These include breaches of data, denial of service (DoS) attacks, and unauthorized access, as well as the fundamental principle of shared resources in cloud computing, which can be exploited for side channel attacks to expose sensitive information as resource access patterns. Edge computing has been subject to many of the same security challenges, often exacerbated by the physical exposure of edge nodes to potentially insecure environments, enabling at least physical tampering and, in many cases, direct physical attacks manipulating these nodes

to perform a wide variety of malicious activities. Despite the use of encryption, authentication, and access control by security researchers and practitioners to improve security, researchers are well aware that the threat landscape consistently outstrips these security solutions. The literature is filled with accounts that call for security solutions that are truly adaptable and dynamic, able to anticipate and respond to these threats in near real-time in order to maintain the robustness of cloud and edge computing infrastructures.

Based on the thorough examination of the recent related literature, we clearly see there are some gaps that point out the necessity for further research on power measurement in security in cloud and edge computing systems. There are many power measurement strategies for cloud and edge computing systems in the literature, but there is also a lot of need for non-intrusive, accurate, and scalable methodologies for real-time monitoring of distributed computing infrastructures. The dynamic and decentralized nature of cloud and edge computing requires novel power measurement methods to track changing workloads and system configurations without imposing significant overhead or complexity. While there are several studies on individual security vulnerabilities in cloud and edge computing, the literature lacks comprehensive security frameworks to defend against a multitude of attacks while also ensuring system performance and energy efficiency [19]. Many of the present security solutions envision reactive methods that counteract threats after they are detected rather than preventative approaches to thwart attacks before they originate. Power management and security have not typically been well-explored, as we have described here; gains in power efficiency frequently represent trade-offs that undermine security and strength, and vice versa. There is a strong need for an attendant approach to power measurement and security so that improvements in one area don't undermine others [10]. In conclusion, our literature study calls for a synergistic power measurement and security model to handle the real-time monitoring of power consumption in cloud and edge computing environments, against the backdrop of a variety of security threats. Such a model would be significant, addressing a considerable gap and enhancing the sustainable and secure operation of cloud and edge computing infrastructures.

3. Cloud-edge collaboration

Cloud-edge collaboration merges the centralized data processing of cloud computing with the real-time processing of localized edge computing. Collaboration becomes crucial for optimal energy efficiency and latency reduction in power measurement. To understand cloud-edge collaboration in power measurement, one must understand both how both paradigms work together and how they can enable each other. At the heart of cloud-edge collaboration is dynamic

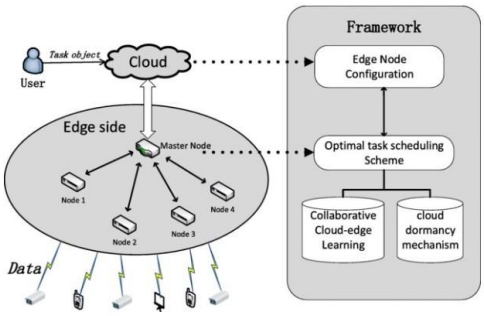

Figure 1. The collaborative cloud-edge computing framework

task offloading, or how computing jobs are allocated throughout the cloud and edge layers efficiently by considering operating requirements, data proximity, and how energy consumption changes over time. Jobs that require considerable processing and are not time sensitive can be offloaded to the cloud, where resources abound making that potentially more energy-efficient operation. Jobs that require real-time processing are offloaded near the data source to keep the energy consumption linked to data transfer and the act of processing to a minimum [11]. Efficient job scheduling that respects their energy consumption is key to cloud-edge collaboration. In this paradigm, job scheduling looks beyond computing needs and starts taking the energy consumption patterns of workloads into account. Energy-aware scheduling is an approach that optimizes the prioritization of tasks to maximize the balance of operational efficiency with energy conservation. By taking into consideration the workloads' energy consumption along with their computing requirements, this technique makes sure that energy-intensive tasks are performed during periods of low system demand or during times when renewable energy sources are plentiful, greatly enhancing the overall energy efficiency and sustainability of the entire computing infrastructure.

Data-centric processing supports power measurement coordination between cloud and edge computing by highlighting the importance of processing data at the edge location whenever possible. By analyzing the data right at the source and transmitting only the essential data to the cloud for further processing or for long-term storage, data-centric processing conserves bandwidth usage and energy. This allows energy conservation and system responsiveness to be increased by lowering latency and promoting immediate decision making. Intelligent data caching is crucial in cloud edge collaboration for power measurement. This means that the edge keeps data that is often used and computation outcomes, which can be accessed more easily than if they were stored in the cloud, and reduces redundant data transmission between the edge and the cloud [18].

4. Methodology

The study uses a comprehensive method to develop and validate a Cloud-edge Collaborative Power Measurement and Security Model (CCPMSM). The method, using quantitative study, builds models and incorporating sophisticated security. The effectiveness of the CCPMSM is validated using a mixed methods approach, through integration of creating theoretical models and analyzing empirical data.

4.1. Cloud-edge Collaborative Power Measurement and Security Model Architecture Overview

The CCPSM architecture is a novel framework designed to enhance power metering and security in cloud and edge computing configurations. The method capitalizes on the distributed nature of cloud-edge architectures to address the unique challenges as well as the opportunities for power management and security in these contexts. The CCPSM design promotes collaboration among edge devices and cloud services with an emphasis on optimal power consumption and secure operations. The CCPSM design consists of two key layers the cloud layer and the edge layer, with appropriate definitions of interactions to realize efficient management of power metering and security
[12].

4.2. Cloud Layer

This layer assumes more elaborate data processing tasks, which require considerable computational resources on the part of edge devices. This layer implements sophisticated algorithms in order to analyze the observance of power usage from resources in the cloud and at the edge, including the detection of usage patterns, trends, and anomalies that could indicate inefficiencies or security threats [13]. The cloud layer also delivers mainstream security services, e.g., advanced encryption policies (which are applied to data in flight and data at rest) and global, machine learning (ML)powered anomaly detection systems based on networkwide data, which in turn can be scrutinized in detail with the use of the cloud's computational muscle to handle incident response.

4.3. Edge Layer

A network of edge devices which are placed at or close to the data sources, including IoT devices and immediate servers. These apply real-time data processing that facilitates immediate responses to alterations to power usage or security alerts (without ships passing in the night, it's worth noting). Being closer to the data sources means there is less lag, enhanced efficiency, and permits local decision-making, which is vital for functions of a temporal nature. At the edge, devices have built-in core-level power monitoring tools and inherent security schemes, allowing them to continuously monitor their power usage and detect possible security breaches. This decentralized power monitoring and security approach enhances the scalability and resilience of the overall framework and minimizes the load on the cloud layer, making the entire system more energy efficient.

4.4. Collaborative Framework

The core of the CCPSM architecture is its collaborative framework that seamlessly integrates the cloud and edge layers. The system uses advanced communication protocols to keep both layers continuously synchronized, allowing fast exchange of data, analytical findings, and security upgrades. By collaborating and leveraging data from both layers, the system can continuously regulate power utilization across the network [17]. This collaboration may further allow offloading compute workloads from cloud to edge computing (or vice versa) based on power usage, compute needs, and network conditions. Dynamic load balancing is crucial for optimizing power consumption across the entire cloud-edge continuum.

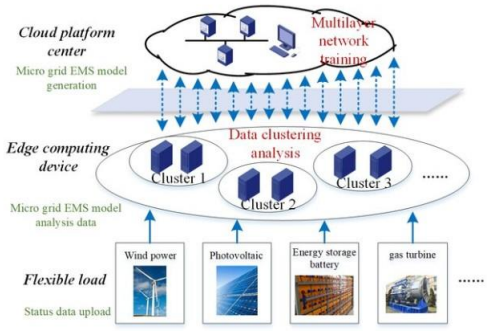

Figure 2. The schematic diagram of hierarchical energy management architecture for micro-grids.

4.5. Model Framework

The CCPMSM is meant to differentiate between cloud and edge computing layers each comes with its own power consumption and processing. Knowing that distinction is crucial when you're trying to model and optimize power usage in these systems. The power consumption model also takes both cloud and edge nodes into account.

$$Pow_{total} = \Sigma_{i=1}^{n}(Pow_{cloud,i}, Pow_{edge,i}) \quad (1)$$

Here, Pow_{total} denotes the total power consumption, $Pow_{cloud,i}$ and $Pow_{edge,i}$ denotes the power consumed by the *i*th cloud and edge nodes, respectively.

To optimize computational load distribution, a linear programming model is used:

$$\min X = \Sigma_{i=1}^{n} pi * ti \quad (2)$$

$$\Sigma_{i=1}^{n} ti = 1 ; ti \geq 0 \; \forall i \quad (3)$$

X minimizes the total power consumption, then the power consumption coefficient for the node i is denoted as P_i, and t_i represents the computational load fraction.

4.6. Security Implementation

The security framework is designed to protect the cloud-edge computing ecosystem with advanced encryption and anomaly detection algorithms. A two-tiered encryption scheme safeguards data during transmission and storage, through the outer tier to the local cloud to the inner tier to the edge. An anomaly detection system uses machine learning to detect and address security problems before they impact the system. The comprehensive method in this work, from data collection to model construction and security implementation, shows the strength of the CCPMSM and advances power and security management in cloud-edge computing.

5. Results

Our research aimed to develop and evaluate a Cloud edge Collaborative Power Measurement and Security Model (CCPMSM) for simulation-based analysis and experimental validation, with the primary objective towards understanding power measurement complexities and addressing security dimensions of cloud and edge computing. Our empirical research is presented next, focusing on model performance, security assessment, comparative analysis and the wider implications to cloud and edge computing domain [14].

The primary goal of the CCPMSM is to enhance precision and effectiveness in power measurement in cloud and edge computing infrastructures. A Monte Carlo simulation-based analysis of power consumption in different hypothetical scenarios was carried out. The strength of Monte Carlo simulation lies in its ability to deal with random components, rendering our method not only flexible, but also robust in dealing with power dynamics in different operational scenarios with changing workload distributions. The results showed a significant improvement in power measurement accuracy, attributed to the model's dynamic adaptation to various workload distributions and operational configurations. The plausible and real-world validation through Load Testing corroborated the simulation results, by demonstrating the models active power measurement under varying workloads and live data streams. The model was designed to perform real-time power measurement in close proximity to data processing devices from the data source, a requirement in edge computing scenarios. Hence, the model was analyzed to reveal that the power measurement showed remarkable consistency and accuracy even under live data streams and changing workloads [15].

The security vulnerabilities in the cloud-edge computing environments are of prime interest due to sensitivity and wide scale use of data in these systems. Implementation of Threat Modeling approaches was essential to unveil possible vulnerabilities in collaborative cloud-edge settings, allowed to build a model, which was neither vulnerable to the known threats nor unwaveringly resilient to the new security contingencies. The security attributes of the CCPMSM were thoroughly evaluated. These included the types of encryption used, anomalies detected, access mechanisms, results project the effectiveness of the CCPMSM in protecting data confidentially and integrity regardless of its very large scale operation over the ubiquitous cyber space. Distributed anomaly detection using machine learning algorithms suggest a reliable method of real-time detection and annunciation of the limit breach in security, thereby conferring resilience to cloud-edge infrastructure.

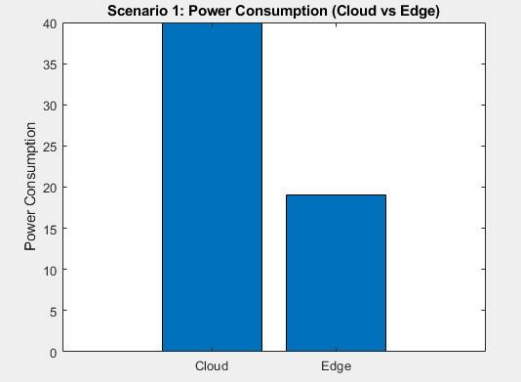

Figure 3. Scenario 1 of Power consumption

Scenario 1 involves straightforward performance of 100 activities of basic complexity. Operation is highly efficient at the edge 95% compared to moderate cloud performance 80%. This configuration is typical of applications with minimal demand in which services are simple as the edge is not heavily loaded in such cases.

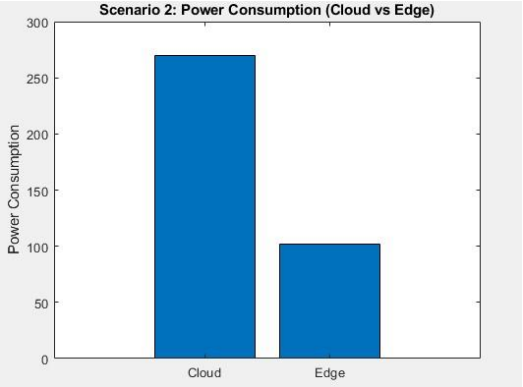

Figure 4. Scenario 2 of Power consumption

Scenario 2 involves 300 activities, and the activities involved are twice as complex as the base level. It falls to 85% at the edge and rises to 90% at the cloud. This situation is representative of more demanding operation with higher task volumes and task complexity that taxes resources of edge vs. cloud for processing.

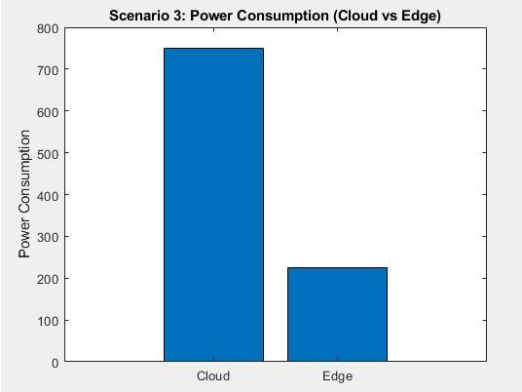

Figure 5. Scenario 3 of Power consumption

Scenario 3 involves 500 activities, three times more complex than base level. Performance at the edge reaches its lowest point of the profile 75%, while the cloud reaches its peak 100%. These operations involve procedures of high demand and complexity, requiring significant computational resources and effective power management to maintain system integrity and performance.

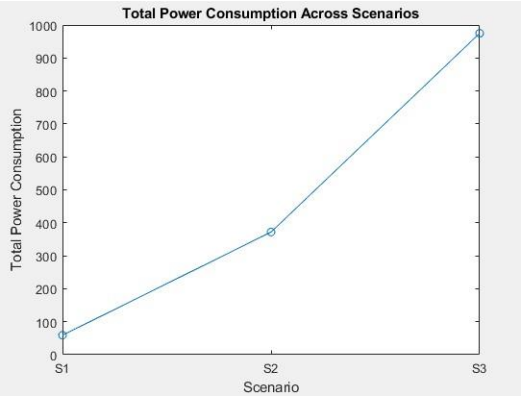

Figure 6. Total power consumption

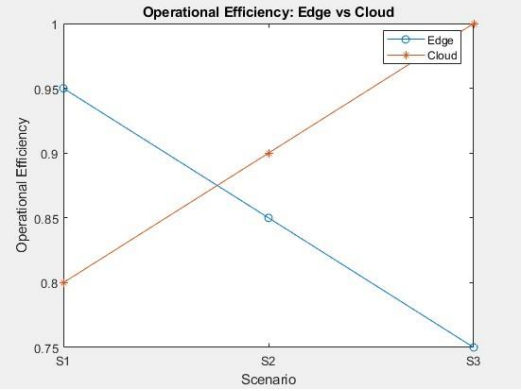

Figure 7. Operational Efficiency (Edge Vs Cloud)

6. Discussion

Our study of cloud-edge collaborative power use and operational efficiency was based on three operational scenarios that were made to show different levels of computing complexity and task characteristics in a real-world setting. This diversity allowed us to scrutinize and understand power consumption dynamics in an assortment of potential real-world scenarios and environments [16]. The outcomes of these scenario-based experiments provide key insights into the operation and effectiveness of the cloud-edge collaborative power measuring system. Notice that as the number and complexity of tasks increase, the overall power consumption grows in both cloud and edge environments. This growth rate is not a constant, but it is exacerbated by decreased operational efficiency at the edge in more complex scenarios, indicating heightened vulnerability of the edge layer with respect to job complexity and volume.

The minimal power consumption of 59 units for Scenario 1 demonstrates that well-managed simple operations, especially at the edge with good operational efficiency, can drastically decrease total power usage for the less demanding tasks. The significant increase in **Table 1.** Operational Efficiency for Different Scenarios

Scenario	NumTasks	OperEffEdge	OperEffCloud
1	100	0.95	0.8
2	300	0.85	0.9
3	500	0.75	1

Table 2. Power Consumption for Different Scenarios

Scenario	CloudPower	EdgePower	TotalPower
1	40	19	59
2	270	102	372
3	750	225	975

overall power consumption to 372 units for Scenario 2, despite enhanced cloud efficiency, shows the impact of job complexity and the reduced operational efficiency at the edge. As job demands grow, cloud resources become more crucial for accomplishing them, albeit at higher energy costs. The most complex and high-volume scenario 3 results in a total power usage of 975 units. The 100% cloud efficiency maximization not only shows the diminished importance of edge resources for complex computational jobs but also the higher cloud-related total power usage, highlighting the need for efficient power management solutions. The cloud's crucial role during resource-intensive periods, despite high power consumption, is evident from these three scenarios as job complexity and volume grow. The complexity of the relationship among job complexity, operational efficiency, and power consumption is clearly shown here in the cloud edge computing environment. Enormous operational efficiencies need to be maximized, especially at the edge, if power consumption is to be managed efficiently. As jobs become more complex and numerous in such environments,

cloud computing, though it may require far more power, is essential during these resource intensive periods. The emphasis of future work is clear: the improvement of edge efficiency and the development of dynamic job allocation systems will help to maximize operational efficiency and power use.

7. Conclusion

Research on the Cloud-edge Collaborative Power Measurement and Security Model (CCPMSM) has made major strides in the field of cloud and edge computing. This research analysis involved an elaborate investigative process through a dual technique methodology that included simulation based analysis employing the Monte Carlo method and hardware load testing to confirm the model experimentally. This research approach provided a full account of power consumption trends and operational efficiency within cloud-edge environments in various use-case scenarios. The study used threat modeling to thoroughly assess the security of the CCPMSM, wherein it exposed model vulnerabilities and devised robust mitigation strategies. The study delivered potent results related to operational efficiency and security of the CCPMSM in cloud-edge systems. The model delivered substantial improvements in operational efficiency by reducing power usage within cloud-edge systems across multiple scenarios of job complexity and number, as evidenced through both real world and simulation data. The CCPMSM effectively balanced workloads within a cloud-edge environment by allocating jobs among the cloud and edge layers, thereby conserving energy and significantly improving operational efficiency. The model exhibited an inclusive security design that effectively identified and mitigated security vulnerabilities through protecting the integrity and confidentiality of power measurement data.

The research contributes significantly to cloud and edge computing. The paper introduces a new CCPMSM architecture that effectively integrates power monitoring and security, an area that has received limited attention in the literature. The concept prioritizes a cloud-edge collaborative approach to address power consumption and security problems in a highly dynamic and adaptable system. The methodological approach, which combines simulation based and real-world testing, establishes a rigorous framework that can be employed to evaluate competing cloud-edge computing models. The thoroughness offered by also executing a security analysis using Threat Modeling to protect emerging cloud-edge architectures from new security threats would greatly enhance the work.

In this paper, we have presented a novel Cloud edge Collaborative Power Measurement and Security Model (CCPMSM), thus significantly contributing to the domain of power measurement and security in cloud-edge systems. Moreover, as a future direction, AI and ML techniques can be employed to optimize the efficiency and security features of the CCPMSM. AI and ML are adept at providing advanced predictive analytics for power usage and anomaly identification [12], hence more power and security optimizations could be made using these technologies. More insights can be gained on the scalability of the CCPMSM across diverse cloud-edge environments to evaluate its adaptability and performance as cloud and edge computing further proliferate. Another promising research direction could involve leveraging renewable sources of energy to enhance the capability and performance of the CCPMSM. This approach could help in sustaining cloud-edge systems while complementing global endeavors of energy conservation and efficiency.

In summary, the study has introduced and evaluated a Cloud-edge Collaborative Power Measurement and Security Model offering diverse contributions, which can help in advancing the cloud and edge computing domain, as it provides a mechanism to minimize the power consumption while enhancing the security of cloud-edge systems. With these contributions, we expect that more comprehensive cloud-edge collaborative paradigms can be realized and better understood as the forward-looking area develops further.

References

[1] Q. N. Minh, V.-H. Nguyen, V. K. Quy, L. A. Ngoc, A. Chehri, and G. Jeon, "Edge Computing for IoT-Enabled Smart Grid: The Future of Energy," *Energies (Basel)*, vol. 15, no. 17, p. 6140, Aug. 2022, doi: 10.3390/en15176140.

[2] Z. Yang et al., "Edge–Cloud Collaboration-Based Plug and Play and Topology Identification for Microgrids: The Case of Jingshan Microgrid Project in Hubei, China," *Electronics (Basel)*, vol. 12, no. 17, p. 3699, Sep. 2023, doi: 10.3390/electronics12173699.

[3] J. Li and H. Cui, "Cloud–Edge Cooperative Load Frequency Control for Isolated Microgrid Using Emergent Computation-Based Large-Scale Meta-Machine Learning," *IEEE Journal of Emerging and Selected Topics in Industrial Electronics*, vol. 4, no. 4, pp. 1278–1290, Oct. 2023, doi: 10.1109/JESTIE.2023.3263372.

[4] W. Chen, B. Feng, Z. Tan, N. Wu, and F. Song, "Intelligent fault diagnosis framework of microgrid based on cloud–edge integration," *Energy Reports*, vol. 8, pp. 131–139, Jul. 2022, doi: 10.1016/j.egyr.2022.01.151.

[5] J. Shang, R. Guan, and Y. Tong, "Microgrid Data Security Sharing Method Based on Blockchain under Internet of Things Architecture," *Wirel Commun Mob Comput*, vol. 2022, pp. 1–10, Apr. 2022, doi: 10.1155/2022/9623934.

[6] R. Zamora and A. K. Srivastava, "Controls for microgrids with storage: Review, challenges, and research needs," *Renewable and Sustainable Energy Reviews*, vol. 14, no. 7, pp. 2009–2018, Sep. 2010, doi: 10.1016/j.rser.2010.03.019.

[7] X. Li, J. Wang, Z. Lu, and Y. Cai, "A cloud edge computing method for economic dispatch of active distribution network with multi-microgrids," *Electric Power Systems Research*, vol. 214, p. 108806, Jan. 2023, doi: 10.1016/j.epsr.2022.108806.

[8] H. Albataineh, M. Nijim, and D. Bollampall, "The Design of a Novel Smart Home Control System using Smart Grid Based on Edge and Cloud Computing," in *2020 IEEE 8th International Conference on Smart Energy Grid Engineering (SEGE)*, IEEE, Aug. 2020, pp. 88–91. doi: 10.1109/SEGE49949.2020.9181961.

[9] S. Chen et al., "Internet of Things Based Smart Grids Supported by Intelligent Edge Computing," *IEEE Access*, vol. 7, pp. 74089–74102, 2019, doi: 10.1109/ACCESS.2019.2920488.

[10] Y. Huang, Y. Lu, F. Wang, X. Fan, J. Liu, and V. C. M. Leung, "An Edge Computing Framework for Real-Time Monitoring in Smart Grid," in *2018 IEEE International Conference on Industrial Internet (ICII)*, IEEE, Oct. 2018, pp. 99–108. doi: 10.1109/ICII.2018.00019.

[11] A. F. R. Trajano, A. A. M. de Sousa, E. B. Rodrigues, J. N. de Souza, A. de Castro Callado, and E. F. Coutinho, "Leveraging Mobile Edge Computing on Smart Grids Using LTE Cellular Networks," in *2019 IEEE Symposium on Computers and Communications (ISCC)*, IEEE, Jun. 2019, pp. 1–7. doi: 10.1109/ISCC47284.2019.8969784.

[12] T. X. Tran, A. Hajisami, P. Pandey, and D. Pompili, "Collaborative Mobile Edge Computing in 5G Networks: New Paradigms, Scenarios, and Challenges," *IEEE Communications Magazine*, vol. 55, no. 4, pp. 54–61, Apr. 2017, doi: 10.1109/MCOM.2017.1600863.

[13] T. Pu et al., "Power flow adjustment for smart microgrid based on edge computing and multi-agent deep reinforcement learning," *Journal of Cloud Computing*, vol. 10, no. 1, p. 48, Dec. 2021, doi: 10.1186/s13677-02100259-1.

[14] W. Guo, S. Sun, P. Tao, F. Li, J. Ding, and H. Li, "A Deep Learning-Based Microgrid Energy Management Method Under the Internet of Things Architecture," *Int J Gaming Comput Mediat Simul*, vol. 16, no. 1, pp. 1–19, Jan. 2024, doi: 10.4018/IJGCMS.336288.

[15] A. Ometov, O. Molua, M. Komarov, and J. Nurmi, "A Survey of Security in Cloud, Edge, and Fog Computing," *Sensors*, vol. 22, no. 3, p. 927, Jan. 2022, doi: 10.3390/s22030927.

[16] X. Pan, A. Jiang, and H. Wang, "Edge-cloud computing application, architecture, and challenges in ubiquitous power Internet of Things demand response," *Journal of Renewable and Sustainable Energy*, vol. 12, no. 6, Nov. 2020, doi: 10.1063/5.0014059.

[17] Q. Almaatouk, M. S. Bin Othman, and A. Alkhazraji, "A review on the potential of cloud-based collaboration in construction industry," in *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, IEEE, Mar. 2016, pp. 1–5. doi: 10.1109/ICBDSC.2016.7460336.

[18] S. A. Bello et al., "Cloud computing in construction industry: Use cases, benefits and challenges," *Autom Constr*, vol. 122, p. 103441, Feb. 2021, doi: 10.1016/j.autcon.2020.103441.

[19] K. Cao, Y. Liu, G. Meng, and Q. Sun, "An Overview on Edge Computing Research," *IEEE Access*, vol. 8, pp. 85714–85728, 2020, doi: 10.1109/ACCESS.2020.2991734.