International Journal of Electrical, Electronics and Computer Engineering **11**(1&2): 01-04(2022)

ISSN No. (Online): 2277-2626

The Convergence of Internet of Things and Cloud Computing: A Review of Architectures, Enablers and Challenges

Rohan Rajoriya[1*] and Jyoti Gupta[2]

[1]Lecturer, Information Technology, Kalaniketan Polytechnic College Jabalpur (M. P.), India.

[2]Lecturer, Electronics & Telecommunication Engineering, Kalaniketan Polytechnic College Jabalpur (M. P.), India.

(Corresponding author: Rohan Rajoriya)*

(Received: 03 December 2021, Accepted: 15 February 2022)

(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: The combination of the Internet of Things (IoT) and cloud computing is an important part of modern digital services. It makes it possible to analyse data from multiple sensing devices at the same time. This review synthesises scholarly work on IoT-cloud integration, focusing on the period preceding widespread Artificial Intelligence at the edge. We trace the architectural evolution from centralised cloud and sensor-cloud models to hierarchical fog and edge computing paradigms, examining key enablers like data management protocols and virtualisation. The analysis identifies persistent challenges in security, interoperability and resource management across the cloud-edge continuum. The main contribution of this work is a unified framework of Pre-AI architectural foundations and technologies, which serves as a clear reference point for the creation of future intelligent systems.

Keywords: Internet of Things (IoT), cloud computing, IoT-cloud integration, Artificial Intelligence

I. INTRODUCTION

The Internet of Things (IoT) envisions a global network of physical objects, each with sensors, actuators and other communication capabilities. (Atzori *et al*., 2010) The sheer volume, velocity, and diversity of data generated by these "things" demands a robust back-end infrastructure. Cloud computing, providing on-demand access to adjustable computing resources such as networks, servers, storage, and applications, naturally became a key component (Mell *et al*., 2011). This convergence, also called the "Cloud of Things" (CoT) or IoT-Cloud, was expected to enable new applications in smart cities, healthcare, industrial automation, smart grids and precision agriculture. This paper examines the main research directions in this convergence.

II. ARCHITECTURAL PARADIGMS FOR IOT AND CLOUD INTEGRATION

Early integration models focused on direct device-to-cloud communication, but limitations in latency, bandwidth, and reliability prompted more hierarchical architectures.

A. Centralised Cloud-Centric Model

The fundamental model, which involves the direct transmission of data from Internet of Things (IoT) devices to cloud platforms like AWS IoT and Microsoft Azure IoT for processing and analysis, was first introduced by (Gubbi *et al*., 2013). Initial research efforts primarily focused on creating efficient communication protocols, such as MQTT and CoAP, tailored for devices with limited resources, as well as the use of RESTful APIs to enable cloud integration.

B. Sensor-Cloud Infrastructure

The Sensor-Cloud model introduced a virtualisation layer that abstracts physical sensor networks to on-demand, scalable cloud services. This "Sensors-as-a-Service" (SaaS) paradigm fundamentally redefined sensor management by decoupling logical sensing tasks from the underlying hardware. Key enabling features included resource virtualisation, which allowed for the dynamic pooling and provisioning of sensor capabilities, and multi-tenancy, which enabled secure, simultaneous data access for multiple applications or users on a shared infrastructure. This abstraction streamlines sensor discovery, administration, and data delivery, significantly improving resource utilisation (Yuriyama & Kushida 2010).

C. Fog and Edge Computing

To tackle the drawbacks of centralised cloud computing, including latency, bandwidth costs, and the inability to work offline, the fog computing paradigm introduced intermediate computational layers between end devices and the cloud (Bonomi *et al*., 2012). Processing capabilities were further extended, encompassing gateways and the devices themselves (Shi *et al*., 2016). The predominant research emphasises architectural configurations, algorithms for service placement, and lightweight containerisation techniques, such as Docker specifically for fog nodes.

III. KEY ENABLING TECHNOLOGIES AND RESEARCH THEMES

A. Data Management and Analytics

Managing the vast amounts of data produced by the Internet of Things (IoT) posed a considerable challenge. Research efforts investigated cloud-based data lakes, time-series databases, and distributed processing frameworks, such as Apache Hadoop and Spark, to support both batch and stream analytics (Chen *et al*., 2014). In addition, Complex Event Processing (CEP) engines were studied to allow for the generation of real-time insights.

B. Virtualisation and Containerisation

The emergence of container technologies, exemplified by Docker, and orchestration systems, including Kubernetes, has facilitated more adaptable deployment and management of microservice-orientated IoT applications across cloud and edge infrastructures, surpassing the capabilities of virtual machines (VMs) (Pahl *et al*., 2017).

C. Communication Protocols

The resource constraints and unreliable networks of IoT environments necessitated efficient, lightweight communication protocols. Message Queuing Telemetry Transport (MQTT), with its publish/subscribe model, and the Constrained Application Protocol (CoAP), a web-transfer protocol for constrained devices, emerged as *de facto* standards for device-to-cloud/edge messaging. Significant research efforts were dedicated to optimising these protocols for low-power operations, handling packet losses, and ensuring security under diverse and challenging network conditions (Al-Fuqaha *et al*., 2015).

D. Semantic Interoperability

To overcome the fundamental challenge of heterogeneity in IoT ecosystems, semantic technologies such as ontologies and the Resource Description Framework (RDF) were proposed. These technologies provide a formal structure for data, enabling machines to interpret context and meaning, thereby facilitating seamless data integration, automated reasoning, and intelligent device cooperation (Perera *et al*., 2015).

V. MAJOR CHALLENGES AND RESEARCH DIRECTIONS

A. Security and Privacy

The vast attack surface created by ubiquitous IoT devices, combined with the centralisation of sensitive data in the cloud, escalated security and privacy concerns to paramount levels. Consequently, research intensified across multiple fronts. These initiatives included developing lightweight cryptographic algorithms suitable for constrained devices, robust mechanisms for secure device authentication and onboarding, end-to-end data encryption for both transmission and cloud storage, and privacy-preserving data aggregation techniques to allow analytics without exposing individual user data (Sicari *et al*., 2015). The distributed nature of fog architectures further complicated these efforts, requiring new trust models and security protocols for the edge-cloud continuum.

B. Standardization and Interoperability

The proliferation of proprietary solutions created significant fragmentation, making a lack of standardisation a critical barrier to scalable, open IoT cloud ecosystems. Heterogeneity in device communication protocols, data formats, and cloud Application Programming Interface (API) designs hindered seamless integration and data exchange. Research, therefore, focused on promoting interoperability frameworks and closely followed the efforts of leading standards bodies and alliances, such as oneM2M, the Open Connectivity Foundation (OCF), and the Industrial Internet Consortium (IIC), which worked to establish common architectures and specifications (Cheruvu *et al*., 2019).

C. Resource Constraints and QoS

Bridging the dichotomy between resource-constrained IoT devices and powerful cloud servers posed a significant systems challenge. A core research direction involved developing intelligent task offloading strategies to decide *what*, *when*, and *where* to offload computational tasks from devices to the edge or cloud. This required network-aware and dynamic scheduling algorithms to optimize for latency, bandwidth, and node availability. Ensuring strict Quality of Service (QoS) and Quality of Experience (QoE) for latency-sensitive applications, like autonomous vehicles or industrial automation, demanded novel management frameworks across the heterogeneous fog layer (Varghese & Buyya 2018).

D. Energy Efficiency

For battery-powered IoT devices, energy consumption, dominated by communication, directly determines operational lifespan. Research pursued optimization at multiple levels: cloud-managed duty cycling protocols to intelligently control device sleep/wake cycles, energy-aware computation offloading decisions that weigh communication cost against processing savings, and the adoption of Low-Power Wide-Area Network (LPWAN) technologies like LoRaWAN and NB-IoT, which offer long-range connectivity with minimal power expenditure.(Ismail *et al*., 2018) These efforts were essential for enabling large-scale, long-term deployments in fields like environmental monitoring and smart agriculture.

VI. DOMINANT APPLICATION DOMAINS

Literature showcased several mature application areas:

A. Smart Cities

Smart city initiatives represent a primary application domain, integrating heterogeneous IoT sensor networks with cloud-based data platforms. Intelligent traffic management systems that analyse real-time vehicle and pedestrian data to optimise signal timing and reduce congestion; smart waste management utilising sensor-equipped bins to optimise collection routes; and structural health monitoring of bridges and buildings through distributed sensor data analysed in the cloud for

predictive maintenance are a few key use cases (Zanella *et al.*, 2014).

B. Healthcare (HIoT)

In healthcare, the IoT-Cloud paradigm has catalysed the advancement of remote patient monitoring and telemedicine. Wearable and ambient sensors continuously collect vital signs, activity levels, and other physiological data from patients. Data is securely streamed to cloud platforms using specialised algorithms, where it is stored, processed, and analysed (Islam *et al.*, 2015).

C. Industrial IoT (IIoT) and Industry 4.0

Industrial IoT (IIoT) is a keystone of the Industry 4.0 revolution, aiming to create smarter, more efficient and autonomous industrial environments. Cloud platforms serve as the central nervous system for IIoT deployments, enabling applications such as predictive maintenance, where sensor data from machinery is analysed to forecast failures before they occur, supply chain optimisation through real-time asset tracking, and the creation of digital twins—virtual, dynamic replicas of physical assets or processes used for simulation and optimisation (Xu *et al.*, 2018). The IIoT is expected to transform how we live, work and play. The critical challenge faced by the Industrial IoT is security and privacy.

D. Precision Agriculture

Precision agriculture uses IoT cloud systems to optimise farming practices, enhancing yield and sustainability. Distributed sensor networks monitor critical parameters such as soil moisture, nutrient levels, temperature, and crop health. This granular, real-time environmental data is transmitted to the cloud for aggregation and sophisticated analysis. (González-Briones *et al.*, 2018).

VII. CONCLUSION

The IoT-Cloud paradigm established itself as a foundational framework for the digital era, leveraging the cloud's processing power to harness data from pervasive IoT sensors. The field's most significant evolution was the architectural shift from a centralised cloud model to a hybrid, hierarchical fog/edge computing continuum, driven by the stringent latency and bandwidth demands of real-time applications. Persistent and critical challenges in security, interoperability, and cross-continuum resource management remained active and unresolved research frontiers, consolidating the architectural progress and technological enablers of this pre-AI phase, this review lays the essential groundwork for understanding the subsequent evolutionary stage: the pervasive integration of artificial intelligence and machine learning across the entire edge-to-cloud spectrum, which makes autonomous and intelligent integrated systems possible, has become the main focus of forthcoming research.

REFERENCES

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, *17*(4), 2347–2376.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, *54*(15), 2787–2805.

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, 13–16.

Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile Networks and Applications*, *19*(2), 171–209.

Cheruvu, S., Kumar, A., Smith, N., & Wheeler, D. M. (2019). IoT frameworks and complexity. *Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment*, 23–148.

González-Briones, A., Castellanos-Garzón, J. A., Mezquita Martín, Y., Prieto, J., & Corchado, J. M. (2018). A framework for knowledge discovery from wireless sensor networks in rural environments: A crop irrigation systems case study. *Wireless Communications and Mobile Computing*, *2018*(1), 6089280.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660.

Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K.-S. (2015). The internet of things for health care: A comprehensive survey. *IEEE Access*, *3*, 678–708.

Ismail, D., Rahman, M., & Saifullah, A. (2018). *Low-power wide-area networks: Opportunities, challenges, and directions*. 1–6. https://doi.org/10.1145/3170521.3170529

Mell, P., Grance, T., & others. (2011). *The NIST definition of cloud computing*.

Pahl, C., Brogi, A., Soldani, J., & Jamshidi, P. (2017). Cloud container technologies: A state-of-the-art review. *IEEE Transactions on Cloud Computing*, *7*(3), 677–692.

Perera, C., Liu, C. H., & Jayawardena, S. (2015). The emerging internet of things marketplace from an industrial perspective: A survey. *IEEE Transactions on Emerging Topics in Computing*, *3*(4), 585–598.

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, *3*(5), 637–646.

Sicari, S., Rizzardi, A., Grieco, L. AS., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164.

Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research directions. *Future Generation Computer Systems*, *79*, 849–861.

Xu, L. D., Xu, E. L., & Li, L. (2018). Industry 4.0: State of the art and future trends. *International Journal of Production Research*, *56*(8), 2941–2962.

Yuriyama, M., & Kushida, T. (2010). Sensor-cloud infrastructure-physical sensor management with virtualized sensors on cloud computing. *2010 13th International Conference on Network-Based Information Systems*, 1–8.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal*, *1*(1), 22–32.