Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 4-A, pp. 1001–1012
DOI : 10.47974/JIOS-1887

Architectural model for Cloud-IoT integration using lightweight open messaging protocol (MQTT)

Amit Kumar Singh Sanger †
Rahul Johari *
Security, Wireless, IoT Network Group of Engineering and Research
University School of Information, Communication and Technology
Guru Gobind Singh Indraprastha University
Sector 16C, Dwarka
Delhi 110078
India

Abstract

The exponential growth of cloud technology and the growing popularity of the Internet of Things (IoT) provide a substantial obstacle in efficiently integrating these technologies to optimize performance and capabilities. It is essential to establish a safe and efficient collaboration between cloud systems and IoT devices in order to optimize daily operations and achieve connectivity objectives. In order to address the challenges, this paper proposes and implements an architectural framework for CloudIoT using the Eclipse IDE. This method facilitates interaction and communication between cloud and IoT systems by making use of the publish-and-subscribe mechanism using the MQTT protocol. An important advantage of this solution is its ability to provide a versatile and expandable framework, which enhances the processing and storage capacities of IoT devices when combined with cloud technologies. Utilizing the MQTT protocol ensures effective and rapid message propagation, resulting in instantaneous communication. Nevertheless, the assessment of its performance is dependent on simulation. Therefore, it is necessary to undertake additional empirical examinations prior to determining its implementation.

Subject Classification: *68M25.*

Keywords: *Cloud computing, CloudSim, Eclipse, Internet of Things, MQTT.*

† *E-mail:* **amitsanger.cse@gmail.com**
* *E-mail:* **rahul@ipu.ac.in (Corresponding Author)**

1. Introduction

The remarkable advances of cloud technology and the Internet of Thing (IoT) has transformed numerous businesses by offering unparalleled capabilities in processing, storage, and communication. Cloud computing provides flexible and easily accessible computer resources that can be adjusted to meet changing needs, resulting in cost savings and enhanced performance. Simultaneously, the IoT has become a vital component for linking and controlling a plenty of devices in several fields, including smart homes, healthcare, business automation, and intelligent and connected cities. CloudIoT integration, the merging of cloud computing with IoT, is revolutionizing the field by improving the effectiveness, expandability, and cognitive capabilities of IoT systems. CloudIoT integration utilizes the extensive capabilities of cloud computing to handle and store vast quantities of data produced by IoT devices. This will offer a highly valuable experience in data analytics, instantaneous decision-making, and remote management of devices, hence greatly enhancing operational efficiency and customer satisfaction.

Integrating Cloud with IoT has an extended application domain. Smart homes provide an efficient management and surveillance of appliances at home, enhancing the convenience and safety of it. Within the health sector, it supports distance patient monitoring and data analysis in delivering healthcare services, contributing to better recovery while also reducing healthcare expenditure. CloudIoT underpins industrial automation through predictive maintenance and process optimization. The concept also applies in creating smart cities with efficient management of resources and public services.

From the perspective of Cloud technology and the IoT framework, the IoT framework is focused on a globally interconnected, dynamically changing infrastructure that supports intelligent, self-configuring nodes. It often consists of little objects with constrained Storage and computational power, and it is defined by real problems with implications for security, efficiency, sustainability, and trustworthiness. Cloud computing, on the other hand, is almost limitless in scope when one takes into account the worldwide availability of data storage and computational resources. Many problems in the Internet of Things were alleviated by this technology. Cloud and IoT are two demanding systems that, when combined, have revolutionized the existence and perspective of network offerings [1].

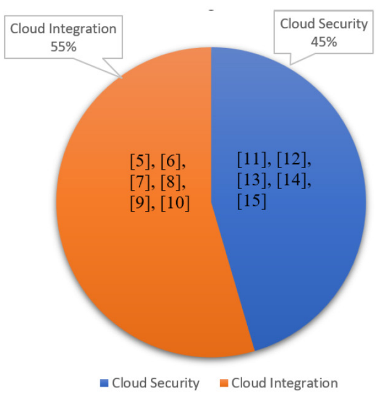
Cloud computing IoT (CloudIoT) refers to the combination of the Cloud and IoT services. IoT and cloud architectures are combined primarily for two primary motivations: First, IoT service providers intend to make use of the features offered by cloud technology, including Self-service-on-demand, high availability, shared resources, instant scalability, and measuring [2]; Second, it is to mitigate the high storage and processing needs of resource-constrained IoT systems [3].

Consequently, IoT systems emerge to be seamlessly incorporated with Cloud systems to provide a consistent foundation for CloudIoT services. This occurrence of combining IoT with the Cloud is also known as CloudIoT [4]. Besides easing resource-constrained behavior and enhancing efficiency, CloudIoT provides a new platform for building and delivering exciting solutions. IoT systems, Cloud technology, and big data are trending together.

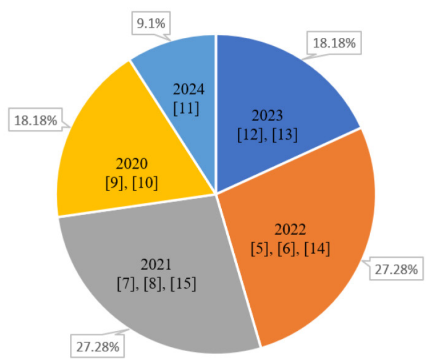
CloudIoT also plays an essential role in the execution of digital twin frameworks by furnishing the necessary infrastructure and offerings for the aggregation, retention, and examination of data originating from IoT devices. This data is indispensable for the establishment and sustenance of precise digital twin representations of tangible entities or systems.

2. Related Work

There were two broad categories—content type and year of publication—into which the reviewed papers fell. The 55% papers dealt with cloudIoT integration and 45% with cloudIoT security, as shown in Figure 1 (a).



(a)



(b)

Figure 1

(a) Chart of papers by category of content type (b) Chart of papers by category of year of publication

In terms of the year of publication, we identified 1 (9.1%) article for 2024, 2 (18.18%) for 2023, 3 (27.28%) for 2022, 3 (27.28%) for 2021, and 2 (18.18%) for 2020, Figure 1 (b). After making sure we have a diverse array of content, we'll review paper that summarizes earlier studies in the CloudIoT domain.

2.1 *CloudIoT Integration*

In [5], the authors examined the amalgamation of cloud technology with the IoT, highlighting the seamless connection between both technologies. It highlighted the benefits, such as scalability, storage, and computational power, that cloud computing brings to IoT systems and examined challenges including data security, privacy, and real-time processing. The article also presented various architectures and models that facilitate the cloud-IoT convergence.

In [6], the authors proposed a multi-cloud integration security framework utilizing honeypots to shore up the security of cloud-based IoT environments. By deploying honeypots, the framework can detect and mitigate potential threats across multiple cloud platforms. The study provided a detailed analysis of the framework's effectiveness in securing cloud IoT systems, focusing on the detection of sophisticated attacks and reducing false positives.

In [7], the authors explored the obstacles and unaddressed aspects associated with the amalgamation of IoT and cloud technology. It delved into the complexities of combining these technologies, such as interoperability, data management, and security. The authors offered a comprehensive review of existing solutions and identified gaps that need to be addressed for more seamless and efficient cloud-IoT integration.

In [8], an overview of the incorporation of IoT and cloud technology, focusing on the technical aspects and potential applications, was presented. It discussed various cloud-based IoT architectures and examined how cloud computing can enhance IoT deployments in terms of scalability, processing power, and data storage. The study also highlighted the key challenges, including latency and security, that must be overcome successfully achieve the full potential of this integration.

In [9], the survey categorized the different paradigms and architectures associated with the cloud-IoT integration. It offered a taxonomy that helps in understanding the various models and frameworks used in this domain. The paper discussed the benefits of cloud-IoT convergence, such as enhanced data processing and scalability, and addressed the associated challenges like security, latency, and interoperability.

In [10], a systematic survey studied IoT and cloud computing integration and analyzed research and methods. The authors examined cloud-IoT technical, operational, and security issues. The survey also noted current trends and future directions and stressed the need for better structures and protocols to promote secure and efficient integration.

2.2 *CloudIoT Security*

In [11], the paper introduced DNACDS, a cloud-based security and access control scheme for IoT and big data environments, leveraging DNA cryptography. The scheme was designed to bolster the safety of cloudIoT systems through the robust encryption methods. The authors analyzed the effectiveness of DNACDS with respect to security, efficiency, and scalability, demonstrating its potential to address the vulnerabilities in cloud-based IoT systems.

In [12], the study proposed a robust framework for cloud computing in sophisticated industrial IoT environments, based on blockchain and Software-Defined Networking (SDN). The architecture aimed to enhance data protection, integrity, and access control in cloud-IoT systems. The paper provided a detailed evaluation of the proposed solution, highlighting its ability to prevent common security threats and ensure reliable communication in industrial IoT settings.

In [13], the paper discussed utilization of IoT and the use of blockchain inside a cloud-based model designed for ensuring safe data transfer in intelligent towns and cities. The authors explored the potential of blockchain to strengthen the security and privacy of data in IoT-cloud environments. This study presented a investigative study of smart city implementation, demonstrating how the proposed model can secure data exchanges and prevent unauthorized access.

In [14], the authors addressed the privacy issues related to the IoT and cloud technology service models, offering a range of suggested solutions. The paper categorized the different security issues, including data breaches, unauthorized access, and privacy concerns, and proposes strategies to mitigate these risks. The study emphasized the importance of adopting a holistic security approach to protect cloud-IoT systems from emerging threats.

In [15], the review provided an overview of the security challenges in cloud-IoT environments. It discussed various attack vectors that targeted cloud-based IoT systems. The paper also explored existing security mechanisms and proposed domains for additional study and innovation for boosting overall safety of cloudIoT systems.

3. Problem Statement

The importance of measuring cloud computing efficiency in the context of IoT integration is growing as a result of the current state of affairs. The expansion of IoT capabilities is inextricably linked to their safe and effective integration. The capacity to measure and enhance the efficiency of cloud computing is becoming increasingly important as more sectors begin to see its potential. Unlocking the full potential of IoT technologies requires ensuring that cloud infrastructure can satisfy the expectations of IoT systems in terms of dependability, scalability, and security. To guarantee a seamless deployment and ongoing operation of connected items and systems in the modern digital era, it is crucial to accurately evaluate cloud computing capabilities inside the IoT framework.

4. Modeling and Simulation Requirements for CloudIoT

4.1 *Communication Protocol for Connection IoT and Cloud*

The MQTT protocol, commonly described as the "Message Queuing Telemetry Transport protocol", is a messaging standard that was developed especially for machine to machine" interaction. MQTT is a lightweight protocol that may be implemented on the TCP/IP as well as features the tiny size of a datagram that allows

for little energy consumption. This protocol is data agnostic, capable of transmitting information in a variety of formats, and employs a publish/subscribe architecture instead of a client-server paradigm. Layered TCP/IP is currently backed by a broad variety of microcontrollers, along with popular market gadget platforms like Raspberry Pi. When it comes to deploying the MQTT protocol on objects, there is a wide variety of choices. For an MQTT network to function as a whole, two primary pieces of software are needed:

- The MQTT Agent must be configured for the device. PAHO client library of Eclipse can be used by a web service that employs Javascript.

- The MQTT Broker manages to publish/subscribe messages. A Linux environment can employ a free broker, including Mosquitto or HiveMQ.

The publish/subscribe method has a feature wherein the message sender and message receiver don't really know one another because of a broker that is separating them. Additionally, time splitting exists, which prevents simultaneous connections between the publisher and the client. As a result, the client keeps receiving data that was initially delayed. Figure 2 portrays the MQTT protocol workflow.

5. System Design

This research provides a framework for combining Cloud and IoT in terms of architectural design. Figure 3 depicts an overview of the system. With the help of request messages sent to a Publisher, Customers can obtain connection to the resources of the data center. The MQTT protocol acts as bridge to link the devices. The devices have the ability to communicate with one another. The broker, that operates in both directions, is one of the essential layers for handling the challenges of data distribution collected or transferred from "things." [16]. It establishes a connection among the Cloud and IoT. This section of the framework provides a collection of computational abstractions to help with the process of integrating and communication of diverse entities. Cloudlets provide remote monitoring and operation of various clients and nodes via the Internet, leveraging network connections. Users are able to manage virtual machines in the data center using this cloudlet.

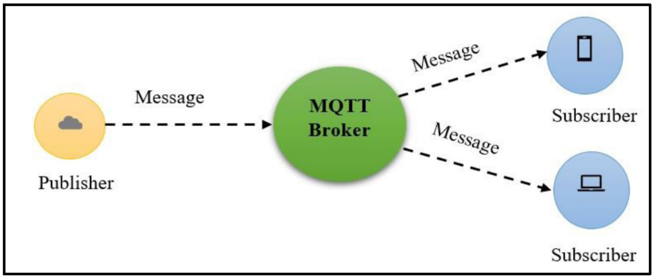


Figure 2

MQTT Protocol Workflows

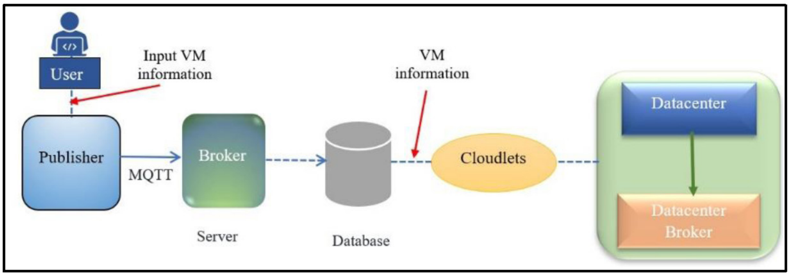


Figure 3

System Design for CloudIoT

6. Algorithm Formulation

Notation

S_r - Server

B_r - Broker where in Br is inside Sr; Sr may contain 1 or more broker

P_r - Publisher

D_t - Database Table

S_{rb} - Subscriber/ Requesting User

T_p - Topic

C_{Rv} - Cloud Resource Values, $C_{Rv} \in$ {Virtual Machine Id, no of CPUs, CPU speed, image, bandwidth, memory size, VM name, Cloudlet ID, length}

$V\,P_r$ - Values Table at Publisher end

$V\,B_r$ - Values Table at Broker end

$V\,S_{rb}$ - Values Table at Subscriber/Requesting User end

T_v - Time at which resources were captured

C_t - Connection Time

M - Message

M_{rp} - MQTT Routing Protocol

I_{sup} - When connection is active

I_{sdown} - When connection is down

C_{id} - Cloudlet ID where C_{id} = 1 to n

The algorithm processes the request for cloud resources made by a broker B_r. It verifies and establishes essential connections between the server making the request (S_{rb}), the broker (B_r), and the publisher (P_r). The VM information is transmitted from publisher to broker, and subsequently from broker to data storage. The system displays suitable notifications

Algorithm 1 Trigger: When S_{rb} requests Cloud Resources from B_r

if $S_{rb}(Is_{up})C_1$ **then**
 $C_1 \leftarrow EstablishConnection(S_{rb})$
 $IsConnectionUp[M_{rp}(P_r, B_r(S_r))]$
 $P_r \leftarrow EstablishConnection(B_r(S_r))$
 if $S_{rb}(I_{sup})C_1$ **then**
  print ("Stale data, obsolete records!!")
  break
 else
 for $\forall$ $S_{ni=1ton}$
  Transfer M(V P_r , V B_r)
  V B_r[ ] receives V P_r[ ]
  Insert M from V B_r into D_t
 end if
 if $S_{rb}(I_{sup}C_1)$ **then**
  Transfer M(V Br,V Srb)
  print ("Connection down between Publisher and Server")
 end if
return
endif

when outdated information is identified or when there is a connectivity problem between the publisher and the server. The program guarantees the integrity of data and manages connections during the utilization of cloud resources.

7. Results

This section provides a high-level summary of the proposed IoT cloud platform. In our experimental MySql has been selected to aid in our database management system development. Finally, the cloudsim is used to allocate a VM for the request made by the users. The Figure 4 (a) – (d) depict the results of the implemented system.

8. Conclusion

In a nutshell, the suggested architectural framework for CloudIoT shows great promise in enhancing the convergence of cloud computing and IoT devices. The puposed framework utilizes the Eclipse IDE and the MQTT protocol for publish-and-subscribe communication. It provides a

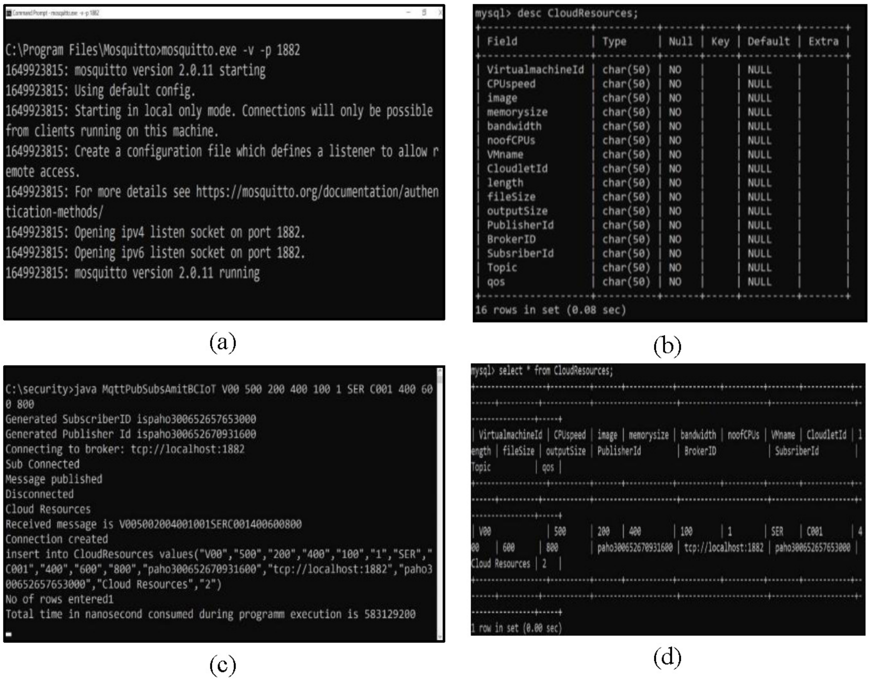


Figure 4

(a) A screenshot illustrating the initiation of the "MOSQUITTO Broker Server" on port number 1882. (b) Screenshot illustrating the schema design of the CloudResources Table designed in MySQL (c) A screenshot capturing the initiation of the Publisher, which advertises the record on the broker window and also insert the record into the Cloud Resources Table (d) Snapshot depicting a MySQL Command Prompt window depicting the record published by the Publisher has been archived into the database.

scalable and adaptable solution that improves the processing and storage capacities of IoT devices. MQTT enables fast and immediate communication between systems by ensuring rapid message dissemination. Nevertheless, as the present assessment relies on simulation, additional empirical investigations are imperative to authenticate its practical application and efficacy in real-life situations. These forthcoming investigations will have a crucial impact in verifying feasibility and efficacy of the framework in tackling the intricate requirements of CloudIoT integration.

References

[1] J. Zhou, T. Leppanen, E. Harjula, M. Ylianttila, T. Ojala, C. Yu, H. Jin, and L. T. Yang, "Cloudthings: A common architecture for integrating the internet of things with cloud computing," in *Proc. 2013 IEEE 17th Int. Conf. on Computer Supported Cooperative Work in Design (CSCWD)*, pp. 651–657 (2013).

[2] M. Mircea, M. Stoica, and B. Ghilic-Micu, "Using cloud computing to address challenges raised by the internet of things," in *Connected Environments for the Internet of Things: Challenges and Solutions*, pp. 63–82 (2017).

[3] Z. H. Ali, H. A. Ali, and M. M. Badawy, "A new proposed internet of things (IoT) virtualization framework based on sensor-as-a-service concept," *Wireless Personal Communications*, vol. 97, pp. 1419–1443 (2017).

[4] N. Nikolov and O. Nakov, "Creating architecture and software of embedded systems with constrained resources and their communication to the IoT cloud," in *Proc. 2019 X National Conference with International Participation (ELECTRONICA)*, pp. 1–4 (2019).

[5] R. Bhatnagar, R. Paramjeet, and G. Amit, *Cloud IoT*, pp. 19–40 (2022). [Online]. Available: https://doi.org/10.1002/9781119813439.ch2

[6] T. Alyas, K. Alissa, M. Alqahtani, T. Faiz, S. A. Alsaif, N. Tabassum, and H. H. Naqvi, "Multi-cloud integration security framework using honeypots," *Mobile Information Systems*, vol. 2022, pp. 1–13 (2022).

[7] I. Abrar, S. N. Pottoo, F. S. Masoodi, and A. Bamhdi, "On IoT and its integration with cloud computing: Challenges and open issues," in *Integration and Implementation of the Internet of Things Through Cloud Computing*, IGI Global, pp. 37–64 (2021).

[8] C. Patil and A. Chaware, "Integration of internet of things, cloud computing," in *IOP Conf. Series: Materials Science and Engineering*, vol. 1022, p. 012099 (2021).

[9] M. Bouakouk, A. Abdelli, and L. Mokdad, "Survey on the cloud-IoT paradigms: Taxonomy and architectures," in *Proc. 2020 IEEE Symposium on Computers and Communications (ISCC)*, pp. 1–6 (2020).

[10] M. Nazari Jahantigh, A. Masoud Rahmani, N. Jafari Navimirour, and A. Rezaee, "Integration of internet of things and cloud computing: A systematic survey," *IET Communications*, vol. 14, no. 2, pp. 165–176 (2020).

[11] A. Singh, A. Kumar, and S. Namasudra, "Dnacds: Cloud IoE big data security and accessing scheme based on DNA cryptography," *Frontiers of Computer Science*, vol. 18, no. 1, p. 181801 (2024).

[12] A. Rahman, M. J. Islam, S. S. Band, G. Muhammad, K. Hasan, and P. Tiwari, "Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT," *Digital Communications and Networks*, vol. 9, no. 2, pp. 411–421 (2023).

[13] L. H. Al-Farhani, Y. Alqahtani, H. A. Alshehri, R. J. Martin, S. Lalar, R. Jain, "IoT and blockchain-based cloud model for secure data transmission for smart city," *Security and Communication Networks*, vol. 2023, Article ID 123456 (2023).

[14] D. K. Saini, K. Kumar, P. Gupta, "Security issues in IoT and cloud computing service models with suggested solutions," *Security and Communication Networks*, vol. 2022, Article ID 123456 (2022).

[15] H. Mahmood, "The security challenges in cloud IoT: A review," *Saudi Journal of Engineering and Technology*, vol. 6, no. 7, pp. 162–168 (2021).

[16] A. K. S. Sanger and R. Johari, "CII-HF: Cloud IoT—Integration hybrid framework," in R. Buyya, S. Misra, Y.-W. Leung, and A. Mondal (eds.), *Proc. Int. Conf. on Advanced Communications and Machine Intelligence*, Springer, Singapore, pp. 387–396 (2023).

Received October, 2024