Comprehensive Journal of Science
Volume (10), Issue (39), (March, 2026)
ISSN: 3014-6266

مجلة العلوم الشاملة
المجلد (10) العدد 39 مارس 2026
ردمد: 3014-6266

Cloud-Based Internet of Things: Technologies, Applications, and Future Perspectives

Thiheebah A. Alwaer

Sabratha University , Economy College ,

thiheebah.abusiriwil@sabu.edu.ly

تاريخ الاستلام:2026/02/01 –تاريخ المراجعة: 2026/02/23– تاريخ القبول: 2026/02/28– تاريخ للنشر : 2026 /03/5

Abstract

The rapid evolution of Internet of Things (IoT) technologies and cloud computing has opened the door for the development of various possibilities for the management and exchange of data among interconnected devices. Cloud computing offers a flexible infrastructure for the management and processing of vast amounts of data from the massive data generated by IoT technologies. On the other hand, IoT technologies have the capability to continuously collect real-time data from different environments and transmit it through the use of various communication networks. The integration of these two technologies offers the possibility for the development of innovative smart services and applications, such as smart homes, intelligent transportation systems, and industrial predictive maintenance. However, the integration of IoT technologies with cloud environments presents various technical challenges, including security and privacy, network, and data management. The paper presents the major aspects of the integration of these two technologies and the various possibilities for addressing the challenges while leveraging the benefits of the integration of these technologies.

1.Introduction .

In recent years, Internet of Things (IoT) has been recognized as a revolutionary technology paradigm, where billions of smart devices are connected through the Internet, enabling data collection, processing, and exchange. IoT devices include various smart technologies, such as sensors, wearable technologies, smart appliances, industrial equipment, and many other intelligent systems, which operate in different environments. The rapid development of IoT technologies has dramatically changed several industries, including the healthcare, transportation, agricultural, and smart cities sectors, through real-time monitoring and intelligent decision-making systems (L. Atzori).

However, the massive amount of data generated through IoT devices requires robust computing infrastructures that can store, process, and analyze large amounts of data. Traditional computing infrastructures have been recognized as having limitations in handling massive data generation through IoT technologies. In this regard, cloud computing has been recognized as an essential technology, which offers storage, computation, and services required to manage IoT technologies (M. Aazam, Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved).

This integration of IoT with cloud computing has the potential to create a robust technological platform where data can be transmitted from smart devices to cloud computing platforms. This integration can enable the development of numerous innovative applications. Some of these applications include smart homes, intelligent transportation systems, industrial automation, and predictive maintenance. Cloud computing can enable IoT systems to allow organizations to take

advantage of numerous benefits, including advanced analytics, real-time monitoring, and decision-making (Dastjerdi, Internet of Things: Principles and Paradigms).

Although there are numerous benefits associated with integrating IoT with cloud computing, there are several technical challenges associated with this integration. Some of these technical challenges include those related to data privacy, cybersecurity, network reliability, and data management. Since data collected from IoT devices can be transmitted and stored in cloud computing platforms, there are numerous concerns regarding data privacy, which are essential considerations for both researchers and practitioners (S. Sicari).

The security risks that exist in cloud-based IoT systems may expose the infrastructure to different types of cyber attacks, including malware injection, data breaches, and information theft. Moreover, the use of traditional security measures, including public key cryptography, in all layers of IoT devices may not be practical due to the low computational capabilities of IoT devices. Other challenges that exist in IoT security include the existence of vulnerabilities in IoT systems, trust concerns in service providers, and interoperability challenges among heterogeneous devices (Evans).

In order to mitigate the challenges that exist in IoT security, researchers have proposed different security measures and technologies that can be implemented in IoT systems to ensure the security and safety of the infrastructure and its users. These security measures and technologies include the implementation of cryptographic protocols, authentication measures, secure communication protocols, and privacy-preserving technologies to ensure the security and safety of critical information in IoT systems. Moreover, improving the reliability of data centers, communication channels, and architectures has become a major research focus in IoT security in recent times. In addition, IPv6 technology is being proposed to improve the interoperability and scalability of IoT systems (Liu).

Furthermore, various security technologies and frameworks have been proposed to improve cloud-based IoT systems, such as secure data sharing, intrusion detection, firewalls, and secure software development. The most prominent solution is the use of risk management frameworks, which help in identifying potential security threats and vulnerabilities while providing strategies to mitigate these risks using policy-based, technical, and organizational security approaches (S. Madakam).

The other significant factor in cloud-based IoT security is the need for transparency and accountability among cloud service providers. The cloud service provider is responsible for providing transparent and clear security policies and protecting the integrity, confidentiality, and availability of user data and infrastructures. Building trust among cloud service providers and users is vital for the successful adoption of cloud-based IoT systems (J. Zhou).

Consequently, the integration of IoT and cloud computing has emerged as an essential research domain in recent years. Several studies have been carried out on various architectures, applications, and solutions regarding the integration of IoT and cloud computing, focusing on improving the efficiency, scalability, and security of these integrated systems. This paper offers an overview of IoT-cloud integration, including applications, benefits, and the major challenges regarding the security and privacy of IoT-cloud integration (al H. A.-F.).

2.Literature Review

The integration of Internet of Things and cloud computing is one of the most discussed topics in recent distributed computing systems. The growing number of devices and volume of data are key factors that have inspired researchers to explore different architectures, frameworks, and technologies for efficient communication and processing of such vast data in IoT-cloud computing systems. Researchers have shown that the integration of IoT and

cloud computing provides efficient infrastructures and resources for complex applications of Internet of Things systems (L. Atzori).

The first term introduced in the context of Internet of Things and cloud computing is CloudIoT. This term represents the integration of cloud computing infrastructures and Internet of Things systems. In CloudIoT systems, cloud computing infrastructures are mainly used for providing efficient services for storing and processing data and deploying applications, while Internet of Things devices are mainly used for sensing and collecting data. Researchers have shown that the unique characteristics of cloud computing and Internet of Things systems are key factors that have inspired the integration of these two technologies for efficient support of Internet applications (al A. B., Integration of Cloud computing and Internet of Things: A survey).

Recent research has been devoted to the architectural models used for developing the IoT-cloud systems. In the conventional cloud-centric model, the collected data from the IoT sensors is sent directly to the cloud servers for storage and processing. Although this model offers high scalability as well as strong computing capabilities, there can be some latency as well as high bandwidth usage in the system for handling the real-time applications (al. L. K.).

To avoid the above limitations of the conventional model, many researchers have proposed different hybrid architectures that integrate cloud computing with edge computing or fog computing. In distributed computing paradigms like edge computing or fog computing, the processing of the collected data from the IoT sensors can be done closer to the IoT devices. Edge computing architectures can be used to provide high data privacy by processing the collected data locally before sending the information to the cloud (al A. A., 2022).

Security and privacy have also emerged as important areas of research for the integration of the Internet of Things and cloud computing. The presence of a large number of devices, diverse modes of communication, and distributed nature of cloud computing have resulted in various security threats and risks. It has been found from various research studies that various cybercrimes, including data breaches, denial of service, and unauthorized access, have the potential to compromise the security of the Internet of Things and cloud computing systems and impact the privacy of the users (al. M. S., 2023).

Thus, various security frameworks and mechanisms have been proposed for the security of the Internet of Things and cloud computing systems. Additionally, various technologies, such as blockchain, artificial intelligence, and machine learning, have also been proposed for the security of the Internet of Things and cloud computing systems (al C. S., 2023).

Another research avenue of significant importance is data management and big data analytics. IoT devices are known to produce massive amounts of data, which must be stored and analyzed in an intelligent way. Cloud computing offers data management infrastructures that can handle big data, thus helping organizations gain useful insights from IoT data streams (al F. C., 2024).

Additionally, recent research has been carried out on the integration of machine learning and artificial intelligence in IoT-cloud computing, with the aim of improving decision-making processes and optimizing system performance. These intelligent systems can analyze large amounts of data, identify anomalies, and provide useful insights, thus improving the performance of IoT systems, especially in smart cities, health monitoring, and industries (al H. K., 2024).

In conclusion, the literature has demonstrated that the integration of IoT with cloud computing has various advantages, such as scalability, computational power, and sophisticated data analytics capabilities. Nevertheless, some challenges persist, such as security threats, latency, interoperability between different devices, and effective allocation

of resources. These challenges are still an area of study in the development of reliable IoT-cloud computing (al. A. M., 2024).

Study	Year	Focus	Key Contribution
Atzori et al.	2010	IoT survey	Overview of IoT architecture and technologies
Botta et al.	2016	CloudIoT concept	Introduced integration paradigm between IoT and cloud
Kong et al.	2022	Edge computing for IoT	Analysis of distributed IoT computing architectures
Sadri et al.	2022	Fog computing	Data reduction techniques in IoT-fog environments
Shirvani et al.	2023	IoT security	Trust-based security models for IoT networks
Surianarayanan et al.	2023	IoT-Cloud security	Analysis of security challenges in integrated systems
Andriulo et al.	2024	Edge-cloud architecture	Comparison of cloud and edge computing for IoT
Kuchuk et al.	2024	Cloud-Fog-Edge integration	Hybrid computing architectures for IoT
Alwakeel et al.	2024	Blockchain trust	Blockchain-based trust management in edge computing
Rupanetti et al.	2024	AI + IoT security	AI-driven security mechanisms
Sheikh et al.	2025	Edge security	Analysis of IoT edge computing threats
Almutairi et al.	2025	IoT-Cloud security	Security threats in cloud-IoT ecosystems
Ahmed et al.	2025	Fog computing	Role of fog computing in IoT systems
Kapoor et al.	2025	IoT applications	Predictive maintenance using IoT devices
Kong et al.	2022	Distributed computing	Integration of IoT with edge systems

Table 1:Comparison of Previous Studies on IoT-Cloud Integration

3.Internet of Things: Concepts and Architecture

Internet of Things (IoT) - It is a term that was first coined by Kevin Ashton in 1998, and it is generally regarded as one of the technologies that can define the future of the Internet and ubiquitous computing (L. Atzori).

This new technology represents a new era of connectivity, where there is communication and data exchange between numerous objects through the Internet. In the IoT concept, "things" represent anything that can be uniquely identified and connected to the Internet. These "things" can range from intelligent objects to non-communicating objects. Some examples of these "things" include intelligent objects, trees, leaves, and beverage bottles.

In IoT-based systems, these objects are considered as information-transmitting nodes, and they communicate with each other through different communication mechanisms, especially Radio

Frequency Identification (RFID) technology. Additionally, there are smart objects present in IoT-based environments, and they may represent physical objects and digital objects that are able to perform specific tasks for humans and their environments. Thus, IoT is not only based on hardware and software concepts but is also based on social interaction and communication concepts (Ashton).

Fig. 1. Internet of Things layers.

The architecture of IoT can be represented using a three-layer model, which includes the perception layer, network layer, and application layer. However, some researchers have proposed an enhanced architecture, which includes the middleware layer and the business layer, in addition to the existing three-layer model (L. Atzori), (Liu). The enhanced IoT architecture is shown in Figure 1, which includes the five layers, namely, the perception layer, network layer, application layer, middleware layer, and business layer.

1. **Perception Layer**

The Perception Layer is the lowest layer in the IoT architecture, and its role is to collect data from the physical world. Data sensing and data acquisition are the functions of this layer, and these functions are carried out through various IoT devices, including sensors, barcode scanners, RFID tags, GPS modules, and cameras. The primary role of this layer is object identification and data acquisition from the surrounding environment (H. Al-FuQaha).

2. **Network Layer**

The Network Layer has the responsibility of transmitting the data received from the Perception Layer to the other layers in the system. The Network Layer in the system can be compared to the network layer in the OSI model. The Network Layer transmits the data from the sensor networks to the Internet using communication means like gateways, wireless networks, or communication protocols. In some instances, the network layer can be made up of network management centers or data processing units.

3**. Middleware Layer**

The Middleware Layer receives data from the Network Layer, and several processes are carried out, including service management, data storage, and information processing. At this layer, the data received is analyzed, and decisions can be made automatically based on the data. After the data is processed, it is sent to the Application Layer for further use (Liu).

4. **Application Layer**

The Application Layer is responsible for providing end users with the processed information in the form of various applications of IoT. This layer offers global management for IoT services and provides application-specific functionalities according to user requirements. Some of the applications of IoT include smart cities, smart homes, smart transportation, vehicle tracking, smart agriculture, and healthcare monitoring, etc. (Liu).

5. **Business Layer**

The Business Layer is concerned with the management of the entire IoT system and the creation of value from the services provided. The data processed by the application layer is converted into meaningful services and business knowledge. This layer analyzes the data to create knowledge, thus contributing to the decision-making process, which may result in better services and economic gains for the service provider.

IoT has also been characterized as Machine-to-Machine (M2M), which is a term used to define the direct communication between two or more machines without the need for a human. The Internet of Things, however, is more than just the conventional definition of Machine-to-Machine communication, as even objects without any previous connection can become part of the IoT using technologies such as barcodes and RFID tags, which can be detected by a device such as a smartphone and connected to the Internet.

4.Fundamentals of Cloud Computing

In recent years, the term Cloud Computing has emerged as one of the most talked-about terms in the field of Information Technology (IT). Cloud Computing is defined as a scalable computing model that uses virtualized resources that can be shared among many users through the Internet. In this computing model, users can use computing services without the need to know anything about the underlying infrastructure. Using the Internet, users can interact with many servers at the same time, and the servers can communicate with each other and exchange information to provide services (Hayes, 2008) (Peter Mell, U.S.Department of Commerce

,Special Publication 800-145).One of the most prominent technological trends is cloud computing, which is mainly attributed to developments in virtualization technology, high-speed networking connectivity, and broadband internet access. Cloud computing is based on existing computing paradigms such as grid computing, utility computing, and autonomic computing. Despite the numerous advantages offered by cloud computing, its adoption as a new technology is also raising some serious concerns regarding its implications on information security and safety.One of the major security concerns related to cloud computing is related to the limited degree of control available to the owners of the data regarding the physical location of their information. Organizations that use cloud computing services often need to depend on the resource allocation, scheduling, and management services offered by the cloud providers, and this may lead to potential security risks. Cloud computing services use different technologies, and these technologies include computer networks, databases, operating systems, virtualization platforms, resource scheduling mechanisms, transaction management mechanisms, load balancing mechanisms, and memory management mechanisms. Thus, any security risks related to these technologies may impact the overall security of cloud computing services. For example, the communication networks used for connecting cloud computing services need to be properly secured to avoid any unauthorized access and attacks ((Kevin Hamlen).

5. **Cloud Computing Architectural Framework**

According to the National Institute of Standards and Technology (NIST), cloud computing can be characterized based on five essential characteristics, three service models, and four deployment models. These are the fundamental components of the operational framework of cloud computing systems, which are often depicted in architectural models such as Figure 2.

In terms of research, cloud computing can be defined as "a model of computing where there is ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources, including networks, servers, storage, applications, and services, which can be rapidly provisioned and released with minimal management effort or service provider interaction."

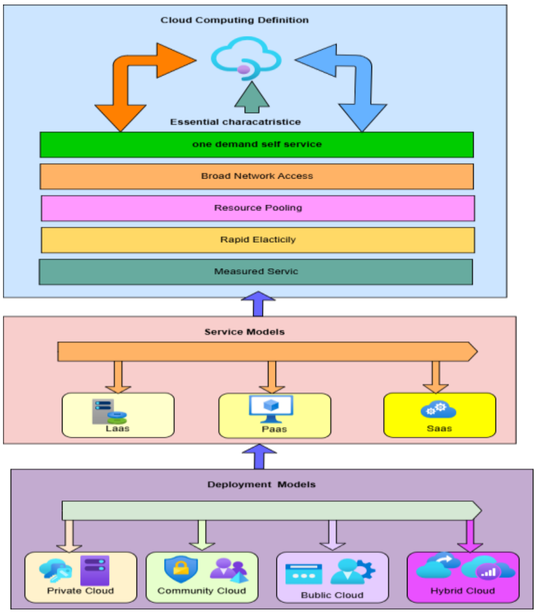

Fig2: NIST Visual Model of Cloud Computing Definition.

A. Essential characteristics of cloud computing

The five key features of cloud computing services include the following, which distinguish it from conventional computing models. These five features describe the operational ability of the cloud services.

- **On-Demand Self-Service:**

The cloud computing service offers the users the opportunity to provision the required amount of server time, storage space, or network services on their own. This can be done on their own without the need for any direct involvement of the service provider.

- **Broad Network Access:**

Cloud services are accessible through standard network mechanisms, allowing users to access them from various devices and platforms. These devices may include smartphones, laptops, tablets, and other thin or thick client systems. This capability ensures that cloud resources can be widely accessed regardless of the device or location.

- **Resource Pooling:**

In the context of the cloud, resource pooling occurs when the service provider pools the resources of the computing infrastructure for the purpose of serving different users. In this case, the resources are pooled in such a way that the users of the services can access the resources of the infrastructure. The resources that can be pooled include the power of the computing infrastructure, the storage infrastructure, the memory of the infrastructure, the bandwidth of the infrastructure, or the virtual machines.

- **Measured Service:**

In the context of the cloud, the measured service occurs when the cloud infrastructure is equipped with the ability to monitor the use of the resources. In this case, the users of the services can monitor the use of the resources such as the storage resources, the power of the infrastructure, the bandwidth of the infrastructure, or the users of the infrastructure.

- **Rapid Elasticity**:

In the context of the cloud, the concept of rapid elasticity occurs when the users of the infrastructure can increase or decrease the resources of the infrastructure. In this case, the users of the infrastructure can access the resources of the infrastructure at any time.

B. Cloud Services Models

The different models of service delivery of the Cloud have been categorized into three archetypal models, with other combinations of these models. These three basic models of Cloud Service are described collectively as the ”SPI Model” where the letters SPI represent Software, Platform or Infrastructure (as a Service), respectively, as described below

Cloud Software as a Service (SaaS) The service provided to the consumer is the ability to use the applications provided on the Cloud infrastructure. The applications that run on the Cloud infrastructure are accessible from different client devices using a thin client, typically a web browser (e.g., email access using the web). The consumer of the Cloud Service does not have control over the underlying Cloud infrastructure, including the network infrastructure, the servers, the operating systems, the storage, or the functionality of the applications themselves, apart from possibly the setting of the application configuration.

- Cloud Platform as a Service (PaaS) The capability provided to the consumer in this case involves deploying consumer-developed or acquired applications created using programming languages and tools supported by the provider into the consumer’s cloud infrastructure. The consumer was not able to manage or control any aspect of the underlying cloud infrastructure including networks, servers, operating systems, or storage but was able to control applications deployed to the cloud infrastructure.
- Cloud Infrastructure as a Service (IaaS) The capability provided to the consumer in this case involves provision of processing, storage, networks, and other basic computing resources to the consumer in which he or she has the ability to deploy and run arbitrary

software including applications and operating systems. The consumer was not able to manage or control any aspect of the underlying cloud infrastructure but was able to control the operating systems, storage, deployed applications, and possibly some aspects of the underlying networking components (e.g., host firewall).

Cloud deployment models

As far as the type of service model used is concerned, there are four different models of deployment for cloud services, and their differences are derived accordingly.

- Public Cloud

It is extremely significant that the cloud infrastructure could be accessed by the public or a large group of organizations and that it belongs to an organization that provides cloud services.

- Private Cloud

The cloud infrastructure is controlled by a single organization. It can be managed by a single organization or a third party and can be on-premises or off-premises.

- Community Cloud

Many organizations have shared a common infrastructure for providing a cloud, and it serves a particular community that has common concerns, such as a mission, security, policy, or compliance. It can be managed by organizations or a third party and can be on-premises or off-premises.

- Hybrid cloud

This cloud infrastructure is composed of two or more clouds, which are private, community, or public clouds, and are still distinct from each other, but are connected or associated with each other by standard or proprietary technologies that facilitate the portability of information and applications, such as cloud bursting, which is used for load balancing between clouds.

6.CLOUD-BASED INTERNET OF THINGS

It is obvious that IoT and Cloud Computing are developing their services. Both technologies have their own characteristics. Considering one side, IoT technology is based on a smart device that is linked in a global network and dynamic infrastructure. IoT technology is characterized by ubiquitous computing. IoT technology is usually characterized by a large number of distributed devices that have limited processing power and storage capacity. Such devices are characterized by problems related to their performance, reliability, privacy, and security (A Botta).

On the other side, Cloud Computing is characterized by a large network that contains vast spaces in terms of abilities and power. To add more, Cloud Computing provides a flexible and robust environment that is used for integrating dynamic data from different data sources (al. J. Z.). Cloud Computing technology has partially solved all problems related to IoT technology. IoT technology and Cloud Computing technology are two differently challenging technologies that are combined to revolutionize the current and future environment for internetworking services (S. M. Babu, A study on cloud based Internet of Things: CloudIoT).

Cloud-based Internet of Things is a platform that enables applications, information, and infrastructure to be used smartly and effectively at a reduced cost. The Internet of Things and Cloud computing are different from each other, but their characteristics are almost complementary, as presented in table 1. This is the reason that most researchers have suggested their integration (A Botta).

7. **Comparison Between IoT and Cloud Computing**

The Internet of Things (IoT) and cloud computing are two emerging technologies in the field of computing that go hand in hand in various computing environments. IoT is focused on

integrating various physical devices and extracting data from the environment using various sensors and smart devices. Cloud computing is a technology that is used for processing a large amount of data generated from IoT applications. Various researchers have highlighted that IoT and cloud computing can be combined to develop intelligent applications in various fields using IoT and cloud computing technologies (L. Atzori), (A Botta).

Feature	Internet of Things (IoT)	Cloud Computing
Definition	IoT refers to a network of interconnected physical devices equipped with sensors and communication capabilities that enable them to collect and exchange data through the Internet (L. Atzori), (H. Al-FuQaha).	Cloud computing is a computing model that provides on-demand access to shared computing resources such as servers, storage systems, applications, and services through the Internet (Grance).
Primary Objective	Collecting real-time data from physical environments using smart devices and sensors.	Providing scalable computing infrastructure for storing and processing large volumes of data.
Main Components	Sensors, actuators, RFID tags, embedded systems, and smart devices.	Data centers, virtual machines, storage systems, servers, and networking infrastructure.
Data Processing Capability	Limited processing power at device level due to hardware constraints.	High computational power capable of processing large-scale data efficiently.
Scalability	Limited scalability depending on device capabilities and communication networks.	Highly scalable due to virtualization and distributed computing technologies (R. Buyya).
Connectivity	Devices communicate through wireless technologies such as Wi-Fi, Bluetooth, Zigbee, and cellular networks.	Services are accessed through the Internet using cloud platforms and service models.
Resource Management	Resources are distributed across multiple devices and gateways.	Resources are centrally managed by cloud service providers.
Security Challenges	Device authentication, physical device vulnerabilities, and data privacy issues.	Data security, multi-tenancy risks, access control, and cloud infrastructure protection (A Botta).
Typical Applications	Smart homes, healthcare monitoring systems, smart agriculture, smart cities, and industrial IoT.	Data analytics, enterprise applications, big data processing, and cloud platforms.

Table 2: Comparison of the IoT with cloud computing.

8.Cloud–IoT Integration Architecture

Cloud computing services have been popularly used in various domains of applications related to the Internet of Things. These domains include genomics data processing, education and e-learning, services for small and medium-sized enterprises, augmented reality applications, manufacturing applications, disaster recovery services, smart cities, digital forensics, hospitality management, e-government services, human resource management, and intelligent transportation systems such as the Internet of Vehicles. The applications of cloud computing

services have helped these applications of IoT to utilize storage and computational services to meet the huge data generated by these applications (A Botta), (H. Al-FuQaha).
While each of the cloud computing and IoT technologies has its own advantage in terms of technical benefits, it has been observed that there are certain technical challenges in deploying these technologies. Some of the technical challenges in deploying these technologies include security concerns, data management issues, interoperability between heterogeneous devices in IoT technology, scalability issues, and effective allocation of resources in IoT technology. As discussed in previous studies, it has been identified that it is a complex research topic to integrate these two technologies due to the requirements of IoT technology and the distributed nature of cloud technology itself (S. Sicari).
In the last few years, the spread of both IoT and cloud computing technologies has been rapid in terms of geographical reach as well as technological development. It has been highlighted by researchers that both technologies have a strong synergistic relationship, as IoT technologies produce large amounts of data that can be efficiently processed through the application of cloud computing technologies. The application of both technologies has the potential to develop intelligent systems that can cater to the needs of real-time systems in different application domains (Dastjerdi, Internet of Things: Principles and Paradigms), (M. Aazam, Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved).
Therefore, different architectural models have been proposed by different researchers to facilitate the integration of IoT devices with cloud computing platforms. The proposed models of architecture seek to facilitate the collection, storage, and processing of data through the sensing capabilities of IoT devices and the computational capabilities of cloud computing platforms. As depicted in Figure 3, the Cloud–IoT architecture comprises different layers that communicate effectively to enhance the efficiency of communication in cloud-enabled IoT environments, including the sensing layer, network layer, and application layer.
Generally, objects that have the ability to sense and collect data from different IoT systems are often controlled or represented using different IoT communication or visualization protocols. The collected data from different objects can also be sent to the cloud for processing and analysis, which makes it easier for data to be managed while at the same time ensuring that the computational performance is enhanced (J. Ren). In the IoT architecture, the application layer is essential in the sense that it can sense environmental information while at the same time sending requests to the cloud infrastructure for the processing of the collected data, obtaining the corresponding results (M. Aazam, Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved).

Fig3 Cloud-IoT Architecture

In addition, the processed information can also be sent back to the IoT systems or other objects for the purpose of carrying out more data analysis or processing tasks. This is often possible since the data can be exchanged between the IoT systems or objects and the cloud infrastructure for the purpose of carrying out more data analysis or processing tasks (R.Gravina), (P. Tan).

In order to enable communication between devices and cloud services over the Internet, various web-based communication protocols are used. Among these protocols, RESTful architecture and SOAP-based web services are used for enabling the interaction between IoT devices and web servers. SOAP-based web services mainly depend on XML-based message passing, and a large number of web services are implemented over the HTTP protocol, which is used for enabling the communication between devices connected over the Internet, as depicted in Figure 4, (S. R. Zeebaree).

In IoT environments where devices are limited and computation capabilities are restricted, a new protocol, known as the Constrained Application Protocol (CoAP), has been introduced, enabling more efficient communication in such environments. The CoAP protocol is based on RESTful principles, and its main advantage is that it is suitable for devices that are limited in processing capabilities and memory size. Moreover, the CoAP protocol is based on the UDP protocol, rather than TCP, which is used in the HTTP protocol, in order to enable more efficient communication in such environments

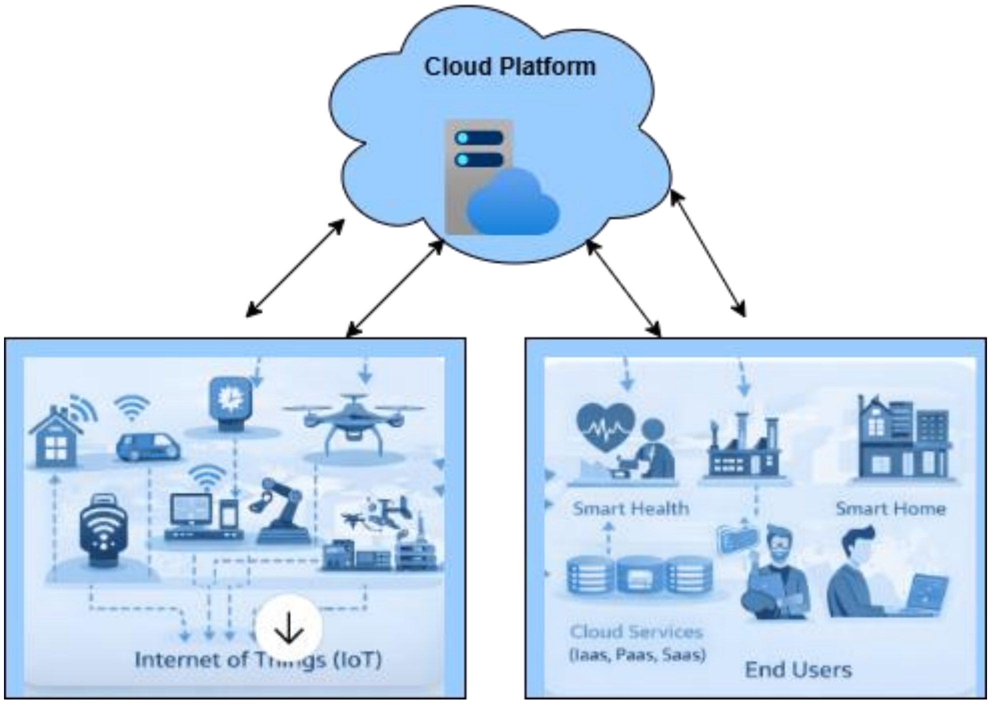

Fig 4: Cloud-IoT Environment.

9. Security Considerations in the Integration of IoT and Cloud Computing

The dynamic changes in Internet of Things (IoT) and cloud computing technologies have greatly affected modern computing environments. Although these technologies were developed separately in the past, their integration has become important due to the benefits it offers. Cloud computing technology has virtually unlimited storage capacity, processing capability, and communication ability, which can be used to improve IoT technology with limited storage capacity, processing ability, and communication ability (A. Botta).

On the other hand, the Internet of Things extends the capabilities of cloud computing since it can connect physical objects, allowing for the collection of real-time data from different environments through distributed sensing devices. For example, in many Internet of Things-based systems, cloud computing infrastructure can be used as an intermediate layer between Internet of Things devices and application services, which can simplify the implementation of such systems, allowing for powerful data processing capabilities. Although there are such advantages, there are also many technical and security challenges associated with the integration of Internet of Things with cloud computing. Some of the challenges include data privacy, service level agreements, data ownership, and the physical location of data, among other concerns. Additionally, there is also the concern of leakage of sensitive data, especially in multi-tenancy-based environments, where traditional security measures such as public key cryptography may not be possible in all layers of Internet of Things-based systems due to the limited computational capabilities of such devices (S. M. Babu, A study on cloud basedInternet of Things: CloudIoT).

The main challenges associated with the integration of IoT and cloud computing are summarized in **Table 3**.

Challenge	Description
Heterogeneity	IoT–cloud infrastructure supports different varieties of devices, operating systems, communication protocols, and platforms. This diversity of technologies makes it difficult for different technologies to integrate with each other seamlessly.
Performance	IoT–cloud applications that need integration often demand Quality of Service (QoS) guarantees. Ensuing the performance requirements for communication latency, computation speed, or storage efficiency can be challenging.
Reliability	However, the reliability of the system assumes importance when the IoT–cloud-based systems are deployed for mission-critical applications, such as smart transportation systems. In such cases, the network connectivity may not be constant, and the devices may not be accessible for short durations.
Big Data Management	This results in a large amount of data being generated, and hence there is a need for scalable cloud infrastructures and data management techniques to store, transmit, and analyze the data.
Monitoring and Management	Continuous monitoring is required in cloud infrastructures to monitor the systems, comply with service level agreements, and monitor the performance and security threats that might arise in the systems.

Table 3: Challenges in IoT and Cloud Computing Integration

There are a number of security threats that may be experienced in the integration of IoT and cloud computing environments. The attacks may impact the availability, integrity, and privacy of the systems and data in the cloud environment (al H. A.-F.) (al A. B., Integration of Cloud Computing and Internet of Things: A Survey). The common security attacks that are experienced in IoT Cloud systems are shown in Table 4

Attack Type	Description	Impact on IoT–Cloud Systems
Distributed Denial of Service (DDoS)	Attackers send a large volume of traffic to overwhelm servers or network resources.	Causes service disruption and prevents legitimate users from accessing cloud services or IoT applications.
Malware Injection Attack	Malicious code is injected into cloud services or IoT devices to alter system behavior.	Compromises data integrity and may allow attackers to control devices or cloud services.
Man-in-the-Middle (MitM) Attack	Attackers intercept communication between IoT devices and cloud servers.	Leads to unauthorized access, data theft, and manipulation of transmitted information.
Data Breach / Data Leakage	Sensitive data stored in the cloud or transmitted by IoT devices is accessed without authorization.	Results in loss of privacy and exposure of confidential information.
Replay Attack	Attackers capture and retransmit valid data packets to gain unauthorized access.	Can manipulate system responses or trigger unauthorized operations.
Unauthorized Access	Attackers exploit weak authentication mechanisms to access IoT devices or cloud services.	Allows attackers to control devices, steal data, or disrupt system operations.
Side Channel Attack	Attackers analyze system characteristics such as timing or power consumption to extract information.	May expose encryption keys or sensitive system information.
Physical Device Attack	IoT devices are physically accessed or tampered with by attackers.	Leads to device compromise, data theft, or malicious firmware installation.

Table 4: Common Security Attacks in IoT–Cloud Systems

10. Research Challenges and Future Directions in Cloud-Based IoT.

Even though there has been rapid progress in Cloud-based Internet of Things (IoT) technologies, there are still some issues that need to be addressed, and research is needed in that area. The issues need to be addressed to ensure that there is a smooth, secure, and scalable integration between IoT devices and cloud computing infrastructures. The major research issues and future directions are discussed in the following sections.

1) Standardization

One of the most important challenges associated with the standardization of Cloud-based IoT systems is still on the agenda. Various studies highlighted the absence of universally accepted standards for integrating IoT devices with cloud infrastructures, which might create significant challenges for the interoperability of IoT services **(Suciu)**. Although various standardization schemes for integrating IoT services with cloud infrastructures have been proposed, significant research is needed for the development of unified architectures, communication protocols, and APIs, which can ensure seamless communication between heterogeneous IoT devices while developing new innovative applications.

2) **Fog Computing**

Fog computing was recently proposed as an extension of cloud computing technology that brings computing resources closer to the edge of the network. Fog computing provides computing, storage, and networking services in a similar way to cloud computing. However, these services are offered closer to IoT devices in order to reduce latency and increase support for real-time data processing. In a fog computing environment, fog nodes are used as an intermediate layer between IoT devices and cloud data centers in order to support delay-sensitive applications that require a quick response time (C. Doukas and I. Maglogiannis). Unlike traditional cloud computing environments, fog computing offers several features that make it suitable for use in IoT applications. Some of these features include location awareness, geographical distribution of computing resources, and reduced latency in the network.

3) **Cloud Capabilities and Security**

Security is a major concern for Cloud-based IoT systems because of the distributed nature of both IoT and Cloud systems. The integration of these systems increases the risk of attack, thus making these systems more vulnerable to cyber attacks. In IoT systems, security measures such as encryption can be employed to ensure data integrity, confidentiality, and authentication. However, some of the challenges facing these systems include issues related to insider attacks and the difficulty of implementing robust security measures on IoT systems, which have limited computational powers (A Botta).

4) **Service Level Agreement (SLA) Enforcement**

Another significant research issue in the context of Cloud-based IoT systems is associated with the enforcement of Service Level Agreements (SLAs). IoT applications require strict Quality of Service (QoS) requirements to be met in terms of data transmission, processing, and storage. Meeting these requirements through a single cloud service provider might be a challenging task, especially in dynamic and large-scale IoT systems. Using multiple cloud service providers could assist in avoiding any violation of Service Level Agreements, thus enhancing the reliability of services. Nevertheless, selecting the optimal combination of cloud service providers dynamically is a complex issue, especially when considering costs, response time, etc., along with the heterogeneity of QoS management mechanisms used in different clouds [56].

5) Big Data

Despite the fact that a number of research studies have been conducted in the field of Big Data, it is still an open challenge in the context of the Cloud-based IoT paradigm and thus needs to be further explored. In the context of the Cloud-based IoT paradigm, the IoT systems produce large volumes of data that are collected from devices located in different geographical locations. This is a challenge in the context of big data management, especially considering the fact that IoT systems often demand real-time processing of the collected data. In this regard, efficient big data management techniques are required to support the processing of the large volumes of data in the context of the IoT systems [57].

6) Security and Privacy

Security and privacy are still significant concerns in the context of Cloud-based IoT systems, which continue to be a significant focus of research. Despite the development of various security mechanisms, these concerns are still not fully addressed. The Cloud-IoT system is sometimes vulnerable to various cyber threats and attacks, which require appropriate security strategies to be employed. Moreover, it is essential to implement appropriate authorization policies and access control mechanisms to ensure that only authorized users are able to access sensitive information. Protecting data integrity, along with user privacy, is a critical requirement in the design of a secure Cloud-IoT system.

7) Energy Efficiency

Energy efficiency is another significant issue in the context of Cloud-based IoT systems. In fact, it has been observed that there are some applications in the IoT domain, which involve the continuous transmission of data between the IoT devices and the cloud infrastructures. In this context, it has been observed that the energy resources of the IoT devices get depleted in a short period of time. In this regard, the issue of energy efficiency is a significant research issue in the context of the IoT domain. Some of the potential solutions, which have been proposed in this context, are data compression, caching, and the reuse of collected data in applications where real-time data is not essential (H. F. Atlam).

. Conclusion

The paper has provided a comprehensive overview of the integration between Cloud Computing and the Internet of Things, with a special emphasis on the complementary nature and the main motivations behind the integration of these two concepts. In this paper, the main focus was on identifying the main security challenges that are presented by the integration between IoT devices and cloud infrastructures, and the potential approaches towards addressing these issues.

The findings of the study revealed the main benefits associated with the integration between Cloud Computing and IoT, which include the benefits in terms of scalability, flexibility, data management, and security. In addition, the paper has discussed a conceptual algorithmic model that is used in addressing the security issues in the context of Cloud-based IoT, as well as the role of encryption in ensuring the security of the data and the communication between IoT devices and cloud services. Despite the significant achievements realized in this field, there is still a need to conduct more research with the aim of establishing more efficient models of integration that will help reduce the security risks while ensuring the high performance of the system. As the Cloud Computing and IoT technologies continue to advance significantly, the need to establish robust models of integration will be vital in the development of the next intelligent Internet-based systems. The integration of Cloud Computing and IoT is a major milestone towards the development of a more connected intelligent ecosystem.

References

(Kevin Hamlen, M. K. (n.d.). Security Issues for Cloud Computing. *Technical Report UTDCS-0210, Department of Computer Science, The University of Texas at Dallas, February 2010, .*

A Botta, W. D. (n.d.). Integration´ of Cloud computing and Internet of Things: A survey. *Futur. Gener. Comput. Syst., vol. 56, 2016, pp. 684–700*.

A. Botta, W. d. (n.d.). On the Integration´ of Cloud Computing and Internet of Things. *2014 International Conference on Future Internet of Things and Cloud, Barcelona, 2014,pp. 23-30.*

al, A. A. (2022). Data reduction in fog computing and Internet of Things.

al, A. B. (n.d.). Integration of Cloud computing and Internet of Things: A survey.

al, A. B. (n.d.). Integration of Cloud Computing and Internet of Things: A Survey. *Future Generation Computer Systems, 2016.*

al, C. S. (2023). Integration of IoT and cloud security challenges.

al, F. C. (2024). Edge computing and cloud computing for IoT.

al, H. A.-F. (n.d.). Internet of Things: A Survey on Enabling Technologies, Protocols and Applications. *IEEE Communications Surveys & Tutorials, 2015.*

al, H. A.-F. (n.d.). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.*

al, H. K. (2024). Integration of IoT with cloud, fog and edge computing.

al., A. M. (2024). Trust management in edge computing environments.

al., J. Z. (n.d.). CloudThings: A common architecture for integrating the Internet of Things with Cloud Computing. *Proceedings of the 2013 IEEE*.

al., L. K. (n.d.). Edge computing-driven Internet of Things: A survey. *ACM Computing Surveys, 2022*.

al., M. S. (2023). Trust-based security in IoT: A survey.

Ashton, K. (n.d.). That 'Internet of Things' Thing. *RFID Journal, 2009*.

Asif Ali Laghari, H. L. (2024). 1- Internet of Things (IoT) applications security trends and challenges, . springer nature.

C. Doukas and I. Maglogiannis. (n.d.). Bringing IoT and cloud computing towards pervasive healthcare. *Proc. - 6th Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput. IMIS, 2012, pp. 922–926.*

C. Stergiou, K. E.-G. (n.d.). Secure integration of IoT and cloud computing,". *Future Generation Computer Systems, vol. 78,pp. 964-975, 2018.*

Dastjerdi, R. B. (n.d.). Internet of Things: Principles and Paradigms. *Morgan Kaufmann, 2016*.

Dastjerdi, R. B. (n.d.). Internet of Things: Principles and Paradigms. *Morgan Kaufmann, 2016.*

Evans, D. (n.d.). The Internet of Things: How the next evolution of the Internet is changing everything. *Cisco Internet Business Solutions Group, 2011*.

Grance, P. M. (n.d.). The NIST Definition of Cloud Computing. *National Institute of Standards and Technology (NIST), Special Publication 800-145, 2011.*

H. Al-FuQaha, M. G. (n.d.). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.*

H. F. Atlam, A. A. (n.d.). An Overview of Risk Estimation Techniques in Risk-based Access Control for the Internet of Things. *in 2nd International Conference on Internet of Things, Big Data and Security, 2017, pp. 1–8.*

J. Ren, H. G. (n.d.). Serving at the edge: A scalable IoT architecture based on transparent computing,. *IEEE Network, vol. 31, pp. 96-105, 2017. 7*.

J. Zhou, Z. C. (n.d.). Security and privacy for cloud-based IoT: Challenges. *IEEE Communications Magazine, vol. 55, no. 1, pp. 26–33, 2017.*

L. Atzori, A. I. (n.d.). The Internet of Things: A survey. *Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010*.

Liu, H. N. (n.d.). Cyber-physical-social thinking space based science and technology framework for the Internet of Things. *Science China Information Sciences, vol. 58, no. 3, 2015*.

M. Aazam, S. Z. (n.d.). Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved. *IEEE Access, vol. 2, pp. 134–152, 2014.*

M. Aazam, S. Z. (n.d.). Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved. *IEEE Access, vol. 2, pp. 134–152, 2014.*

P. Tan, H. W. (n.d.). Teaching management system with applications of RFID and IoT technology. *Education Sciences, vol. 8, p. 26, 2018.*

Peter Mell, T. G. (U.S.Department of Commerce ,Special Publication 800-145). The NIST Definition of Cloud Computing ,The National Institute of Standard and Technology.

R. Buyya, J. B. (n.d.). Cloud Computing: Principles and Paradigms. *Wiley, 2011*.

R.Gravina, P. A. (n.d.). Multi-sensor fusion in body sensor networks: State-of-the-art and research challenges,. *Information Fusion, vol. 35, pp. 68-80, 2017*.

S. M. Babu, A. J. (n.d.). A study on cloud based Internet of Things: CloudIoT. *2015 Global Conference on Communication Technologies (GCCT), 2015, pp. 60-65.*

S. M. Babu, A. J. (n.d.). A study on cloud basedInternet of Things: CloudIoT. *2015 Global Conference onCommunication Technologies (GCCT), 2015, pp. 60-65.*

S. Madakam, R. R. (n.d.). Internet of Things (IoT): A literature review. *Journal of Computer and Communications, vol. 3, no. 5, pp. 164–173, 2015.*

S. R. Zeebaree, K. J. (n.d.). Impact analysis of SYN flood DDoS attack on HAProxy and NLB cluster-based web servers,. *Indones. J. Electr. Eng. Comput. Sci, vol. 19, pp. 510-517, 2020.*

S. Sicari, A. R.-P. (n.d.). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, vol. 76, pp. 146–164, 2015*.

Suciu, G. S. (n.d.). Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things. *19th Int. Conf. Control Systems and Computer Science (CSCS)2013, pp. 513- 518.*