International Journal of Cloud Applications and Computing
Volume 13 • Issue 1

Integration of the Internet of Things and Cloud:
Security Challenges and Solutions – A Review

Chellammal Surianarayanan, Centre for Distance and Online Education, Bharathidasan University, India*
Pethuru Raj Chelliah, Reliance Jio Pvt. Ltd., India
https://orcid.org/0000-0001-5220-0408

ABSTRACT

The integration of IoT and cloud poses increased security challenges. Implementing security mechanisms in IoT systems is challenging due to the availability of limited resources, large number of devices, heterogeneity of devices, generation of bulk data, etc. Likewise, cloud resources are also vulnerable to security issues due to virtualization, insider threats, data loss, data breaches, insecure APIs, etc. Security is of major concern with the integration of IoT and cloud. The primary objective of this review is to highlight the security issues associated with an IoT system and cloud system and with the integration of the two, as well as to highlight solutions in each case. The secondary objective is to describe popular IoT-cloud platforms and also to highlight how such platforms facilitate secure integration. Ultimately a highlight on a shared responsibility model of implementing security is emphasized as both IoT users and cloud service providers have to cooperatively share the responsibility to deploy secure cloud-based IoT applications.

KEYWORDS

Cloud Security, IoT-Cloud Platforms, IoT-Cloud Security, IoT Security

INTEGRATION OF THE INTERNET OF THINGS AND CLOUD: SECURITY CHALLENGES AND SOLUTIONS: A REVIEW

The Internet of Things (IoT) sensors purposefully interact with other connected entities in the real world to acquire different operational parameters and share the data to other devices and systems over the Internet or any other communication network without human intervention (Mercado Herrera et al., 2023). The advancement in hardware and wireless communication technologies promotes the usage of IoT devices across various domains. In 2025, the number of IoT devices in the world will be approximately 75.44 billion (Alam, 2018). Artificial intelligence (AI) makes the IoT networks intelligent and increases the scope of IoT connectivity and vast data streams (Khanam et al., 2022). The rapid growth of IoT sensors and the corresponding generation of a large volume of data are obviously in need of huge resources for storage and processing (Qabil et al., 2019). There are several popular

DOI: 10.4018/IJCAC.325624 *Corresponding Author

approaches like on-premises private clouds and edge device clouds for data capture, storage, analysis, and visualization. But with the public cloud environment (off-premises, on-demand, and online) emerging as the most optimized and affordable option for large-scale data storage and processing, IoT data gets transmitted over the Internet to faraway cloud centers. There are automated tools for data storage, analysis, management, observability, and maintenance in the public cloud environment.

With its rapid and flexible resource provisioning at low cost (Truong & Dustdar, 2015) cloud can fulfill the major deficiencies of IoT, namely limited storage, low computing power, and deficient processing capabilities (Atlam et al., 2017; Botta et al., 2016). Cloud can provide the required scalability to an application while allowing the provisioning of resources to instantly scale up or down according to the demands of the applications (Righi et al., 2020). Machine learning tools and platforms that are available in public cloud make descriptive, predictive, prescriptive, and adaptive analytics easier (Adi et al., 2020). Rough set theory can efficiently select optimized cloud services for different tasks, namely inductive reasoning, automatic classification, pattern recognition, learning algorithms, and data reduction (Tiwari & Garg, 2022). Cloud provides monitoring and management of remote IoT sensors (Lineswala & Swali, 2020) in a centralized manner along with a robust Identity Access Management (IAM). Also, it offers services to store the security credentials of IoT devices.

Already IoT has revolutionized the way that different industries like healthcare, manufacturing, agriculture, oil and energy, transportation, and logistics are enhancing their processes by using IoT technology. In addition, cloud computing assists the IoT systems by providing adequate resources and ensures business continuity. Ultimately, the integration of IoT and cloud has led to the development of various useful applications like smart grid automation, smart energy, smart city, transportation and logistics, manufacturing, healthcare, agriculture (Alam, 2021; Dahiya et al., 2022; Guida et al., 2021; Haghnegahdar et al., 2022; Khattab et al., 2016; Xu et al., 2023).

In short, the integration of IoT and cloud provides the following benefits:

1. The IoT devices can access hardware and software services from cloud from any remote location.
2. Cloud enables centralized device registration, configuration, and management.
3. The scalability of cloud-based IoT applications is very high.
4. Cloud provides secure storage facility and life cycle management for IoT data.
5. Cloud can serve as a platform for developing complex applications with better use of online data.
6. Cloud facilitates large scale data analysis using machine learning algorithms.
7. Could ensures regular updates of software, platforms, and firmware which protect the IoT applications against known vulnerabilities.
8. Cloud provides scalable, reliable, and adaptable services and solutions which certainly lead to enhanced performance of the real-life applications.

Despite the above benefits, the integration of IoT and cloud is implicitly associated with two limitations, namely latency and the need for high network bandwidth for the transfer of data from IoT to cloud. Due to the network latency, real-time analysis of IoT data is not possible with faraway cloud environments. Real-time analytics are performed using edge computing at the point of data acquisition itself. But irrespective of the situations in which real-time analysis is required, for any application, the relevant and necessary data must be archived for deeper analysis, decision making, data warehousing, business continuity, and business intelligence purposes. Since data is one of the primary assets of corporations it cannot be ignored without extracting hidden knowledge from it. This illustrates the frequent need for cloud computing resources by IoT applications.

Apart from the above benefits, the amalgamation of IoT and cloud is associated with increased security issues (Almolhis et al., 2020). Security becomes the major concern when an IoT system is integrated with cloud due to reasons like improper device updates, lack of robust protocols, lack of device monitoring, not updating the default passwords and unconscious use (Tawalbeh et al., 2020). Also, the built-in authentication mechanism of IoT devices is not reliable due to weak, guessable,