Chapter 6
Best Practices:
Adopting Security Into the Cloud–Based Internet of Things

Anchitaalagammai J. V.
Velammal College of Engineering and Technology, India

Kavitha S.
Velammal College of Engineering and Technology, India

Murali S.
Velammal College of Engineering and Technology, India

Padmadevi S.
Velammal College of Engineering and Technology, India

Shanthalakshmi Revathy J.
https://orcid.org/0000-0003-1724-7117
*Velammal College of Engineering and Technology, India*

ABSTRACT

The internet of things (IoT) is rapidly changing our society to a world where every "thing" is connected to the internet, making computing pervasive like never before. It is increasingly becoming a ubiquitous computing service, requiring huge volumes of data storage and processing. Unfortunately, due to the lack of resource constraints, it tends to adopt a cloud-based architecture to store the voluminous data generated from IoT application. From a security perspective, the technological revolution introduced by IoT and cloud computing can represent a disaster, as each object might become inherently remotely hackable and, as a consequence, controllable by malicious actors. This chapter focus on security considerations for IoT from the perspectives of cloud tenants, end-users, and cloud providers in the context of wide-scale IoT proliferation, working across the range of IoT technologies. Also, this chapter includes how the organization can store the IoT data on the cloud securely by applying different Access control policies and the cryptography techniques.

Figure 1. Illustration of Cloud based IoT
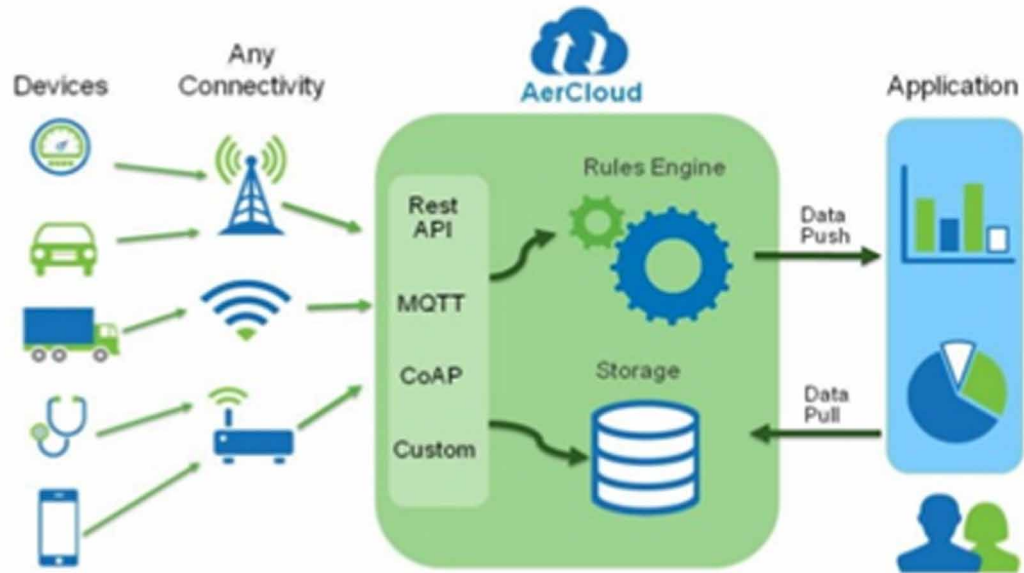
INTRODUCTION

IoT is an interconnection of everyday objects in a network, which are usually equipped with tremendous intelligence level. IoT has increased the usage of Internet gigantically by integrating every object for inter-action through embedded systems, which leads to a highly dispersed network of devices communicating with human beings as well as electronic devices which support internet. IoT is a promising phenomenon which will improve the quality of our lives. In the recent past, IoT has been the center of attraction of researchers and practitioners from all over the world. IoT is a device which is capable of capturing data, storing and processing it. It can also visualize services, monitor and manage various devices.

There is a need of an advanced prototype for security, which considers the security issues from a holistic perspective comprising the advanced users and their intercommunication with this technology. Internet is primary of IoT hence there can be security loophole. Intercommunication paradigms are developed based on sensing programming for IoT applications, evolving an intercommunication stack to develop the required efficiency and reliability. Securing intercommunication is a crucial issue for all the paradigms that are developing based on sensing programming for IoT applications(Choudhury et al., 2017). If we provide good software which insures about security of the cloud storage system and communication between IoT device and cloud, then there is a no problem to accept cloud storage to store IoT data.

Data generated by the IoT devices is massive and therefore, traditional data collection, storage, and processing techniques may not work at this scale. Furthermore, the sheer amount of data can also be used for patterns, behaviors, predictions, and assessment. Additionally, the heterogeneity of the data generated

Related Content

IoT and Blockchain in Indian Perspective
Dipti Chauhanand Jay Kumar Jain (2021). *Blockchain Applications in IoT Security (pp. 186-202).*
www.irma-international.org/chapter/iot-and-blockchain-in-indian-perspective/261887

Fog Computing Architecture, Applications and Security Issues
Rahul Newareand Urmila Shrawankar (2020). *International Journal of Fog Computing (pp. 75-105).*
www.irma-international.org/article/fog-computing-architecture-applications-and-security-issues/245711

Empowering Agriculture With Conversational AI: An Application for Farmer Advisory and Communication
Mrignainy Kansal, Pancham Singh, Mili Srivastavaand Prateek Chaurasia (2023). *Convergence of Cloud Computing, AI, and Agricultural Science (pp. 210-227).*
www.irma-international.org/chapter/empowering-agriculture-with-conversational-ai/329136

An Extension of the MiSCi Middleware for Smart Cities Based on Fog Computing
Jose Aguilar, Manuel B. Sanchez, Marxjhony Jerezand Maribel Mendonca (2018). *Fog Computing: Breakthroughs in Research and Practice (pp. 230-250).*
www.irma-international.org/chapter/an-extension-of-the-misci-middleware-for-smart-cities-based-on-fog-computing/205979

Automate Model Transformation From CIM to PIM up to PSM in Model-Driven Architecture
Yassine Rhazali, Asma El Hachimi, Idriss Chana, Mohammed Lahmerand Abdallah Rhattoy (2020). *Modern Principles, Practices, and Algorithms for Cloud Security (pp. 262-283).*
www.irma-international.org/chapter/automate-model-transformation-from-cim-to-pim-up-to-psm-in-model-driven-architecture/238912