Data Access and security in Cloud integrated IoT

Dr.THOMAS FELDMAN
Assistant Professor, Dept. of CSE
Chirstu jyothi Institute of Technology & Science
jangaon, India.

PROF.MUSILEK
Assistant Professor, Dept. of CSE
Chirstu jyothi Institute of Technology & Science
jangaon, India.

*Abstract-**Cloud computing and Internet of Things (IoT) are two very different technologies. Cloud computing involves delivering data, applications, photos, videos, and more over the Internet to data centers. The Internet of Things, meanwhile, refers to the connection of devices to the Internet. Cloud structures including storage of device data, analytics, process management for IoT system, visualization of data, host components for device management including a device registry. Cloud structure is bi directionally connected with IoT system by Internet technologies using wired and wireless networks. Network connection is direct to the public network. The Internet of Things (IoT) involves the internet-connected devices we use to perform the processes and services that support our way of life. Another component set to help IoT succeed is cloud computing, which acts as a sort of front end. In this paper we discuss the data collection and access methods of IoT devices with cloud integration.***

Keywords: *IoT, cloud computing, security.*

I. INTRODUCTION

Cloud Computing and Internet of Things (IoT) are two emerging field in modern internet era. Their massive adoptions and use in day to day life are expected to increase in future, making them important components of the future internet. Most of the papers proposed the model for cloud and IoT separately. IoT [1] is generally characterized by real world and small things with limited storage and processing capacity which has the consequential issues regarding reliability, performance, security and privacy. At the same time, cloud computing has virtually unlimited capabilities such as storage, processing power, privacy and security. Cloud computing provides infinite computation and storage through a shared pool of resources, which can be dynamically allocated and easily obtained by any IoT application. This paper discusses the new architecture which solves IoT issues by integrated with cloud platform. The figure 1 shows the architectural views of IoT combined with Cloud computing. Cloud structures including storage of device data, analytics, process management for IoT system, visualization of data, host components for device management including a device registry. Cloud structure is bi directionally connected with IoT system by Internet technologies using wired and wireless networks. Network connection is direct to the public network. Communication technology helped to power consumption and low range method using Bluetooth, WiFi, 2G, 3G and 4GLTE. IoT backbone structure connects IoT end point devices to the internet or public network. IoT end points contain a sensing system which used to gather the information about the environment.

A) Internet of Things

The Internet of Things (IoT) is a term coined in 1999 by Kevin Ashton, a British technology pioneer working on radio-frequency identification (RFID), to describe a system where the physical world is connected to the Internet via ubiquitous sensors. Since then, although IoT has become a very hot topic in industry and academia, there is still no standard universally-accepted model for the IoT [2]. For example, the definition for high complexity IoT system from IEEE is:"Internet of Things envisions a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration. The International Telecommunication Union (ITU) focuses more on the communication aspect of IoT and defines it as: "A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" [12].

Figure1. IOT system

B) Security and Privacy concerns in IoT

However, as each coin has two sides, there is a downside to IoT: when everything is connected, everything is at risk. Theoretically, any Internet-connected device can be hacked. More connected devices mean more attack vectors and more possibilities for adversaries who are attracted by the tremendous economic benefits and scale of IoT systems [6]. With enormous benefits brought by IoT, IoT devices [7] also make organizations and individuals vulnerable. Generally speaking, the attack surfaces that cause the security and privacy issues fall into two categories:

- Attacks on IoT Device Level
- Attacks on IoT Application Data

II. A COMMON ARCHITECTURE FOR INTEGRATING THE INTERNET OF THINGS WITH CLOUD COMPUTING

Jiehan Zhou et al [3] focus on a common approach to integrate the Internet of Things and Cloud Computing under the name of Cloud Things Architecture. Cloud Things architecture, Cloud-based Internet of Things platform which accommodates Cloud Things [3] IaaS, PaaS, and SaaS for accelerating IoT application, development, and management. Cloud based [8] internet of things different than conventional Internet of Things is basically the ability to develop, deploy, run, and manage things applications online via the cloud. Cloud based IoT platform and their interaction with the three cloud computing models of Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Fig.2 shows Cloud Things [4] architecture is an online platform that allows system integrators and solution providers to leverage a complete Things application infrastructure for developing, deploying, operating, and composing things applications and services that consist of three major modules:

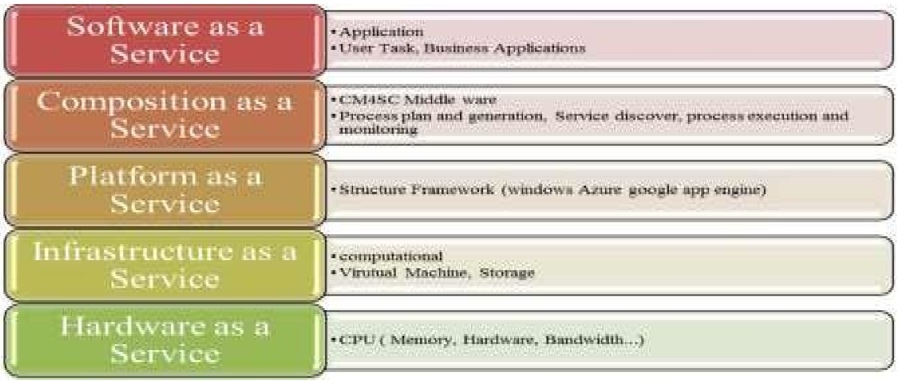

Figure2. Cloud architecture for dynamic service

The Cloud Things service platform for Things is a set of Cloud services (IaaS), allowing users to run any applications on Cloud hardware. The Cloud Things service platform for Things dramatically simplifies the application development [11], eliminates need for infrastructure development, shortens time to market, and reduces Things management and maintenance costs. The Cloud Things service platform offers users unique device management capabilities [9]. It communicates directly with devices and provides storage to collect Things data and transmit Things events. Vast amount of sensor data can be processed, analyzed, and stored using the computational and storage resources of the Cloud. The Cloud Things service platform allows sharing of sensor resources by different users and applications under a flexible usage mode. The Cloud Things Developer Suite for Things is a set of Cloud service tools (PaaS) for Things application development. These tools include open Web service application programming interfaces (APIs), which provide complete development and deployment capabilities to Things developers. The Cloud Things [5] Operating Portal for Things is a set of Cloud services (SaaS) that support deployment and handle or support specialized processing services including service subscription management, community coordination, Things connection, Things discovery, data intelligence, and Things composition [10].

III. IOT SENSORS WORKING

Let's take one example of the IoT based navigation system which guide to the user by giving the speech based instruction for navigating through the aware and unaware environment. IoT based navigation system follows the client-server methodology, in which, the smart phone (android) considered as the client and the server is capable to provide the navigation directions for the multiple user at time. IoT based navigation system designed and developed by C-DAC pune as Proof of Concept (PoC) phase of NISG. This system consist 3 Linksys WRT54g Wi-Fi access points and Samsung galaxy S2 mobile phone. In this system, received signal strength indicator (RSSI) based fingerprinting technique in Wi-Fi is used for IoT arrangement. The received signal strength of each access device is measured and stored to find out the exact location. The calculation for determining the exact location of the individual is done in two phases; training phase and tracking phase. In training phase, signal strength is measured from different location to provide the correct location to the server as the radio map. During the tracking phase multiple users are connected to the server by using smartphones. Then online data is matched with offline location data and based on this navigation, instructions are given to the specific user. To improve the exact location and correct navigation different routing algorithms and advanced navigation can be combined.

IV. TO MAINTAIN THE SECURITY OVER THE IOT DATA

IoT architecture can be represented with the help of four types of interconnected systems such as things, gateways, network and cloud.

- **Things:** Today there are large numbers of things available in industrial and commercial settings. Now a day, they acquire home and mobiles also. Already cars, many device sensors, mobile phones access the internet through the wireless network. IoT environment requires such type of things which are intelligent and capable to filter the data as well as manage this data and they are easy to connect with gateways. For examples: mobile phones, security alarm at home, smart buildings and industrial automation.
- **Gateways:** Many of the designed things are not capable to connect with the internet. For solving this issue gateway is used as intermediate between the internet and things.
- **Network Infrastructure:** Internet is a worldwide structure of interconnected IP networks that links billions of computers together. Network infrastructure comprises routers, gateways, switches, repeaters, and many other devices which controls the data traffic and connect with cable and telecom networks handled by different service providers.
- **Cloud:** Cloud contains large pools of virtualized servers and servers connected together. To support the IoT environment cloud infrastructure runs different applications which are capable to analyze the data collected from different devices and sensors to make the correct decision.

In the IoT Architecture, IoT devices are placed to collect the data, if devices are not able to connect to the internet and cannot transfer the data, and then gateways are used as intermediate between things and cloud to provide the needed connectivity. In the designed secure system, the administrator will define the roles according to the job functionalities played in the organization, and then he/she adds the user in the system who wants to access the stored data from the cloud storage according to their needs. Administrators also create one role manager and give access rights to manage the roles of the user. The Role Manager allocates the specific roles to the user and has authority to remove the role assigned to the user. After that, the collected data from devices are encrypted by the administrator and stored it in to the cloud storage for the particular role so that only the users with appropriate roles can decrypt and view this data. The data collected from IoT devices is stored in encrypted format, therefor cloud provider is not able to see or read this data.

V. CONCLUSION

The combination of cloud computing and IoT will enable new monitoring services and powerful processing of sensory data streams. For example, sensory data can be uploaded and stored with cloud computing, later to be used intelligently for smart monitoring and actuation with other smart devices The cloud effectively serves as the brain to improved decision-making and optimized internet-based interactions. However, when IoT meets cloud, new challenges arise. There is an urgent need for novel network architectures that seamlessly integrate them. The critical concerns during integration are quality of service (QoS) and quality of experience (QoE), as well as data security, privacy and reliability. Cloud computing offers a practical utility-based model that will enable businesses and users to access applications on demand anytime and from anywhere.

REFERENCES

[1] Tan, Lu, and Neng Wang. "Future internet: The internet of things." 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). Vol. 5. IEEE, 2010.
[2] Aazam, Mohammad, et al. "Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved." Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th-18th January, 2014. IEEE, 2014.
[3] Zhou, Jiehan, et al. "Cloudthings: A common architecture for integrating the internet of things with cloud computing." Computer Supported Cooperative Work in Design (CSCWD), 2013 IEEE 17th International Conference on. IEEE, 2013.
[4] Distefano, Salvatore, Giovanni Merlino, and Antonio Puliafito. "Enabling the cloud of things." Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on. IEEE, 2012
[5] Hassani Bijarbooneh, Farshid. "Cloud-Assisted Data Fusion and Sensor Selection for Internet-of-Things." (2015).
[6] O. Harfoushi, B. Alfawwaz, N. Ghatasheh, R. Obiedat, M. Abu-Faraj and H. Faris, Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review, *Communications and Network*, vol. 6, no. 1, pp. 15–21, (2014).
[7] J. D. Bokefode, S. A. Ubale, S. Apte Sulabha and D. G. Modani, Analysis of DAC MAC RBAC Access Control based Models for Security,*International Journal of Computer Applications*, vol. 104, no. 5, October (2014).
[8] B. W. Lampson, Protection, *ACM SIGOPS Operating System Review*, vol. 8(1), pp. 18–24, January (1974), J. K. Wang, Xinpei Jia, DataSecurity and Authentication.
[9] Rahul Bhadoriya,Manju K.Chattopadhyay and Prakash W.Dandekar, ―Low Cost IoT for Laboratory Environment‖,2016 Symposium on Colossal Data Analysis and Networking(CDAN),978-1-5090-0669-4/16.2016 IEEE.
[10] Sharma, Kamlesh, and T. Suryakanthi. "Smart system: Iot for university." Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on. IEEE, 2015.
[11] Singh, Jatinder, et al. "Twenty security considerations for cloud-supported Internet of Things." IEEE Internet of Things Journal 3.3 (2016): 269-284.
[12] L. Wang and R. Ranjan, "Processing Distributed Internet of Things Data in Clouds," IEEE Cloud Computing, vol. 2, no. 1, 2015, pp. 76–80.