Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 06, No. 04, December 2020.

CLOUD OF THINGS: ARCHITECTURE, RESEARCH CHALLENGES, SECURITY THREATS, MECHANISMS AND OPEN CHALLENGES

Shamsul Haq, Adil Bashir and Sahil Sholla

(Received: 13-Jun.-2020, Revised: 9-Aug.-2020 and 6-Sep.-2020, Accepted: 9-Sep.-2020)

ABSTRACT

In this era of communication and networking technology, Internet of Things adds to the existing technological era and brings revolution to the Information Technology world. Internet of Things consists of interconnected devices which may be digital, physical or mechanical devices equipped with unique identifiers and having the capability to transmit the sensed information to other devices autonomously. Internet of Things is recognized as being composed of resource constraint devices in terms of processing competency, storage capacity and power resources. To cope up these constraints, existing computing technology known as cloud computing can be used to facilitate the Internet of Things system by offloading its processing and storage requirements. In this paper, we have provided the necessity and benefits of Cloud and IoT integration. Further, the paper has identified several research issues that arise due to Cloud-IoT integration. Among the several research issues, it was observed that security and privacy concerns are pivotal in Cloud-IoT integration and need to be addressed to make the integration successful. The core security and privacy threats have been identified and the existing security mechanisms have also been researched in this paper. The paper also highlights open security and privacy research issues in the Cloud-IoT paradigm. This paper can act as a baseline for the research that is needed in the area of security and privacy issues in the Cloud-IoT or Cloud of Things paradigm.

KEYWORDS

Internet of things, Cloud computing, Cloud of things, Security, Privacy, Encryption algorithms.

1. INTRODUCTION

Internet of Things (IoT) is a networking paradigm that connects billions of heterogeneous devices, called Things, within the same backbone, essentially, the Internet. These connected things sometimes referred to as objects, have the ability to generally capture environmental data using dedicated sensors, process the acquired data and communicate the data with other things, within the framework of a smart application [1]. According to the definition of Internet Architecture Board (IAB), IoT is a network of smart things and a way of intelligent communication among an enormous number of connected devices that use a new version of internet protocol (IPV6) providing 2^{128} unique addresses, capable of realizing the actual concept Internet of Things. IoT is swiftly growing and is expected to connect billions of objects in the near future, which requires billions of network addresses. The IoT in whole can be said as an innovation to put together smart things, frameworks and sensors [2]-[4]. The basic building blocks of IoT include hardware, embedded programming and wireless communication technologies. The core of any IoT infrastructure is billions of interconnected devices containing sensors and actuators to sense or detect any physiological or environmental phenomenon. Notwithstanding, to transmit the information that the devices gather, these devices require handling and processing abilities, so that the data can be structured and formatted for transmission. This handling and processing function is commonly performed by a micro-scale integrated circuit; for example, a System-on-a-Chip (SoC) or a Field-Programmable Gate Array (FPGA). Since IoT devices are embedded devices, they are prototyped using competitive micro-scale platforms; for example, Arduino, Phidgets and Raspberry Pi. Prototyping IoT devices using these platforms requires micro-scale controller programming, circuit construction abilities and profound knowledge of hardware communication standards, such as I2C or SPI, that are used to build communication between the micro-scale controller and the associated sensors and actuators. The embedded programs are regularly developed using computer programming languages such as C, C++, Python and JavaScript.

S. Haq, A. Bashir and S. Sholla are with Department of Computer Science and Engineering, IUST, Awantipora, J&K, India. Emails: s.haq266@gmail.com, adilbashir.445@gmail.com and sahilsholla@gmail.com