Application Domains, Evaluation Data Sets, and Research Challenges of IoT: A Systematic Review

Ritika Lohiya and Ankit Thakkar, *Member, IEEE*

***Abstract*—We are at the brink of Internet of Things (IoT) era where smart devices and other wireless devices are redesigning our environment to make it more correlative, flexible, and communicative. IoT is now evolving to Internet of Everything, as it incorporates and builds a system that includes wireless networks, sensors, cloud servers, analytics, smart devices, and advanced technologies. The IoT systems are equipped with embedded devices having network connectivity and sensors to have a machine-to-machine interaction. The field of IoT is advancing to provide smart solutions to various applications, such as transportation, healthcare, farming, to name a few. Considering the diverse perspective of IoT systems/network, this article aims at discussing different applications of IoT across various research domains and to highlight the use of IoT in a variety of applications. We have systematically reviewed applications of IoT with the data sets to understand the characteristics of the data collected by the IoT devices. In this article, a comprehensive survey on the role of IoT in various application domains is presented for the years 2015–2019. This article lists different commercialized solutions developed in various IoT application domains. The aim to discuss commercialized IoT paradigms is to highlight research efforts performed in the field of IoT that have been transformed into real-life solutions. This article also discusses research challenges in the field of IoT to strengthen the research for developing future IoT applications.**

***Index Terms*—Challenges, future research directions, Internet of Things (IoT), IoT applications, IoT data sets, security.**

I. Introduction

INTERNET of Things (IoT) is a regime that consists of millions of smart devices connected to analyze and influence our day to day activities. IoT records one of the fastest growth rates in the domain of computing technologies, with an estimation of 5.3 billion global Internet users and more than three times of the global population of devices connected with each other by the year 2023 [1]. This proliferation of connected devices in an operating environment has developed a platform known as IoT. A platform consisting of sensors and devices that integrate smoothly with the environment to interact and share information. The scope and impact of computing is also pervasive in IoT systems. IoT includes personal, enterprise, automation, and cloud computing services that brings together diversified research domains, such as security, energy efficiency, system infrastructure, data analysis, and application development [2]–[4]. The broad scope of IoT challenges various aspects of applications, such as computation and connection. For instance, an IoT device deployed in a network will require energy efficiency, interoperability with software interface, and security of data [3]. Therefore, it is a tedious task to fulfill all the requirements while considering software as well as hardware issues of an IoT application. However, addressing the requirements of an IoT application pertaining to software and hardware provides an opportunity to collaborate and execute interdisciplinary research [5].

An IoT system/network consists of devices/nodes connected with each other for communicating and sharing information. Each of the device/node is recognized by using a unique identifier that can be addressed globally [6]. The amount of information that can be accessed for identifying a device/node can be as low as static data that is stored on the radio frequency identification (RFID) tags [7]. Therefore, the IoT system/network is referred to as system/network with objects having unique identifier and Internet connectivity. The development in the field of IoT is fueled by its increased use in various domains, such as wireless sensor networks (WSNs), healthcare, agriculture, home appliances, and enterprise networks [8]. Thus, with the expansion in communication networks, the number of physical devices used and the information that can be shared through Internet has been increased [9].

There exists ubiquitous connectivity among a variety of IoT devices, services, and applications that include devices, such as computers, smart phones, and sensors, services, such as Android-based mobile applications, Web services, and cloud services, and applications, such as wireless enabled cars, lighting systems, heating and ventilation enabled air conditioners, smart-home applications, to name a few [10]. These devices, services, and applications are called as IoT-enabled as they present in the network and are able to communicate with other devices. There are different types of communication technologies that are used for establishing communication and connection between devices, services, and applications. For instance, 3G, LTE, Wi-Fi, Bluetooth, ZigBee, Z-wave, and Sigfox are few of the communication network technologies that provide connectivity and communicating services for IoT deployment on different platforms [10], [11].

By scrutinizing and considering various application areas and technologies of IoT, U.S. National Intelligence Council has listed IoT in "Disruptive Civil Technologies" with a potential impact on U.S. national power by the year 2025 [12].

Manuscript received September 12, 2020; revised November 10, 2020; accepted December 28, 2020. Date of publication December 31, 2020; date of current version May 21, 2021. *(Corresponding author: Ritika Lohiya.)*

The authors are with the Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad 382481, India (e-mail: 18ftphde30@nirmauni.ac.in; ankit.thakkar@nirmauni.ac.in).

Digital Object Identifier 10.1109/JIOT.2020.3048439