Chapter 26
SEF4CPSIoT Software Engineering Framework for Cyber-Physical and IoT Systems

Muthu Ramachandran
https://orcid.org/0000-0002-5303-3100
Leeds Beckett University, UK

ABSTRACT

Cyber-physical systems (CPS) have emerged to address the need for more efficient integration of modern advancement in cyber and wireless communications technologies such as 5G with physical objects. In addition, CPSs systems also needed to efficient control of security and privacy when we compare them with internet of things (IoT). In recent years, we experienced lack of security concerns with smart home IoT applications such as home security camera, etc. Therefore, this paper proposes a systematic software engineering framework for CPS and IoT systems. This paper also proposed a comprehensive requirements engineering framework for CPS-IoT applications which can also be specified using BPMN modelling and simulation to verify and validate CPS-IoT requirements with smart contracts. In this context, one of the key contribution of this paper is the innovative and generic requirements classification model for CPS-IoT application services, and this can also be applied to other emerging technologies such as fog, edge, cloud, and blockchain computing.

INTRODUCTION

Cyber-Physical Systems (CPS) and the Internet of Things (IoT) is on the rapid increase as the demand for such applications is growing exponentially. There is a very strong reason for connecting three technologies such as CPS, IoT, and Cloud as the first two are connected to a cloud for receiving and analysing data. Cloud computing has emerged to provide a more cost-effective solution to businesses and services while making use of inexpensive computing solutions that combines pervasive, Internet, and virtualisation technologies. Cloud computing has spread to catch up with another technological evolution as we have witnessed Internet technology which has revolutionised communication and information superhighway.

DOI: 10.4018/978-1-6684-7132-6.ch026

Cloud computing is emerging rapidly and software as a service paradigm is increasing its demand for more services. However, this new trend needs to be more systematic with respect to developing secure software engineering and its related processes such as requirements, design, development, and test. For example, current challenges that are faced with cybersecurity are: application security flaws and lessons learned which can all be applied when developing applications for CPS and IoT systems. Similarly, as the demand for cloud services increases and so increased importance sought for security and privacy. Cloud service providers such as Microsoft, Google, Salesforce.com, Amazon, GoGrid are able to leverage cloud technology with a pay-per-use business model with on-demand elasticity by which resources can be expanded or shortened based on service requirements. CPS and IoT combined have great potential to evolve new applications such as smart homes, smart cities, smart roads, smart transports, smart grids, etc. Let us take, smart home which can connect several devices such as smart home security cameras, smart home monitoring systems with machine learning to predict abnormalities, smart detection sensors to detect movement in the house when you are away, smart speakers such as Alexa, Google Home, and Siri, smartphone apps connected to home energy supply, smart kitchen utensils such as smart fridge, smart dishwasher, smart oven, smart heating systems, smart radiator valve, etc. However, existing work on smart home applications by Varghese & Hayajneh (2018), Hu, Yang, Lin, & Wang (2020), & Yassein, Hmeidi, Shatnawi, Mardini, & Khamayseh (2019) reported that "the current security mechanisms are insufficient as developer mistakes cannot be effectively detected and notified due to lack of applying systematic software development principles".

There are varying definitions and understanding of these two terms found in the literature as follows:

Alur (2015) defines CPS as:

A CPS system is defined as a system consists of computing devices communicating with one another and interacting with the physical world via sensors and actuators. Examples of such systems include smart buildings to medical devices to automobiles.

Whereas (Lin, 2017) defines a CPS system as the interactions between cyber (means sensing, computing, and communicating using current technologies such as Bluetooth, Wifi, etc.) and physical components and also aims to monitor and control the physical components (external world).

McEwen and Cassimally (2014) defines IoT as:

An IoT system consists of any physical objects contains controllers, sensors, and actuators that are connected with the Internet. Examples of such systems include any devices capable of sending and receiving data through the internet such as internet-enabled washing machines, dishwashers, etc.

Whereas (Lin, 2017) defined IoT as a networking infrastructure to connect a massive number of smart devices and to monitor and control devices and IoT forms a horizontal layer support for a vertical layers of CPS connecting a range of applications such as smart city services requires smart transportation, smart energy, smart weather forecasting, smart grid, and smart government councils, etc.

In addition, (Ray, 2018) provides a more systematic review of IoT architectures consisting of components of IoT devices such as connectivity, memory interfaces, processor, graphics, audio and video interfaces, storage interfaces, and i/o interfaces (sensors, actuators, etc.) and also discusses Gartner's prediction

Related Content

An Effective and Computationally Efficient Approach for Anonymizing Large-Scale Physical Activity Data: Multi-Level Clustering-Based Anonymization

Pooja Parameshwarappa, Zhiyuan Chenand Gunes Koru (2020). *International Journal of Information Security and Privacy (pp. 72-94).*

www.irma-international.org/article/an-effective-and-computationally-efficient-approach-for-anonymizing-large-scale-physical-activity-data/256569

Dataveillance in the Workplace: Privacy Threat or Market Imperative?

Regina Connolly (2015). *Handbook of Research on Emerging Developments in Data Privacy (pp. 69-84).*

www.irma-international.org/chapter/dataveillance-in-the-workplace/123526

Face Recognition Technology: A Biometric Solution to Security Problems

Sanjay K. Singh, Mayank Vatsa, Richa Singhand K. K. Shukla (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications (pp. 3968-3999).*

www.irma-international.org/chapter/face-recognition-technology/23339

Analyzing Newspaper Articles for Text-Related Data for Finding Vulnerable Posts Over the Internet That Are Linked to Terrorist Activities

Romil Rawat, Vinod Mahor, Bhagwati Garg, Shrikant Telang, Kiran Pachlasiya, Anil Kumar, Surendra Kumar Shuklaand Megha Kuliha (2022). *International Journal of Information Security and Privacy (pp. 1-14).*

www.irma-international.org/article/analyzing-newspaper-articles-for-text-related-data-for-finding-vulnerable-posts-over-the-internet-that-are-linked-to-terrorist-activities/285581

Edge-to-Edge Network Monitoring to Detect Service Violations and DoS Attacks

Ahsan Habib (2009). *Handbook of Research on Information Security and Assurance (pp. 179-192).*

www.irma-international.org/chapter/edge-edge-network-monitoring-detect/20649