Chapter 2
Security of the Tomorrow's Cyber Physical Systems

Ankur Biswas
Adamas University, India

Abhishek Roy
Adamas University, India

Priyadarshini Tikader
Vidyasagar University, India

Dharmesh Dhabliya
https://orcid.org/0000-0002-6340-2993
Vishwakarma Institute of Information Technology, India

Kirti H. Wanjale
https://orcid.org/0000-0003-4271-504X
Vishwakarma Institute of Information Technology, India

Sabyasachi Pramanik
https://orcid.org/0000-0002-9431-8751
Haldia Institute of Technology, India

Ankur Gupta
https://orcid.org/0000-0002-4651-5830
Vaish College of Engineering, India

EXECUTIVE SUMMARY

The industrial sector has emerged as a hub for research on the quickly emerging field of smart technology throughout the last few decades. Smart technology (ST) included a wide range of cutting-edge technologies, such as block chains, artificial intelligence, cyberphysical production systems, internet of things, industrial internet of things (IOT), and systematic data analysis. The authors provide an overview of numerous smart technologies that may be used to control the complex properties of computer and sensor technologies, with the goal of reducing the gap between people and robots. This chapter presents the whole literature evaluation on the use of ST to enhance the production and maintenance of machinery and equipment, as well as

DOI: 10.4018/979-8-3693-2675-6.ch002

potential risks to ST. This chapter also includes the survey report that compares the adoption rate of the current technology to that of the previous five years in an effort to lower the amount of human labor needed in the industrial sector by utilizing a variety of sensors, affordable techniques, and real-time results.

INTRODUCTION

Numerous themes are causing major change in CPSs: increased integration of the IoT. The IoT, that is the technique of linking physical objects to the internet via the use of sensors and other devices, is becoming more integrated with it. One of the most significant future advances in cybersecurity is the usage of AI and ML technology. Large data sets may be analysed by these clever algorithms, which can also spot patterns or abnormalities that can point to a possible cyberthreat. CPSs combine sensing, computing, and network to attach physical architecture and entities to the Internet and to each other. NSF is at the forefront of driving advancements in the fundamental knowledge and abilities required to implement cyber-physical systems. The three main components of a CPS are a distributed cyber system, a networking and transmission element, and a physical system, as seen in Figure 1. The architecture of CPSs consists of distributed hardware, software, and network components integrated in physical systems and surroundings. They combine cyber (computation and communication) and physical (sensors and actuators) capabilities. CPS is used in almost every sector and environment, including building systems, manufacturing, aerospace, electric power grids, healthcare, and automobiles. The three Cs of ideal security are coordinated, integrated, and all-encompassing. Cybercriminals are always devising new tactics to prey on huge organizations, governments, and compact and mid-extension organizations. The protection of data, software, and hardware on internet-connected devices against cyberthreats is known as cybersecurity.