Chapter 17
Cyber Security: New Realities for Industry 4.0 and Society 5.0

Atharva Deshmukh
https://orcid.org/0000-0002-8039-3523
Terna Engineering College, India

Disha Sunil Patil
Northeastern University, USA

Gulshan Soni
School of Engineering, O.P. Jindal University, India

Amit Kumar Tyagi
https://orcid.org/0000-0003-2657-8700
National Institute of Fashion Technology, New Delhi, India

ABSTRACT

Industry 4.0 is a new industrial revolution based on the deployment of billions of internet of things (IoTs) devices. With this industrial revolution, Society 5.0 is also taking place (introduced and applied in Japan). These revolutions are dependent on one another in order to improve productivity, transparency, security, and trust, among other things. However, when IoTs communicate over the internet and store their data on a cloud/remote server, there is a risk of security breaches. Hackers can also attach/steal these systems or the data they hold by leveraging smart devices/artificial intelligence. When the internet of things (IoTs) and machine learning (ML) collaborate, they coin the phrase automated analytics, which means analytics by intelligence or artificial intelligence.

DOI: 10.4018/978-1-6684-6697-1.ch017

INTRODUCTION

Manufacturers must adopt new architectural models that integrate technology, people, regulations, and procedures. They may now have several physical factories spread across several geographies. These must be able to communicate and work in a secure environment." As a result, implementing a Zero Trust architectural paradigm is critical. Today's production floors and supply networks are more open. We need granular visibility and controls to prevent unauthorized users, apps, and data from accessing the network. We must also recognize that, despite these safeguards, nothing is flawless and those dangers can still enter. We'll need safeguards in place to identify and prevent assaults rapidly. For example, solutions that use machine learning to automate threat detection and response for IoT and Industry 4.0. The same technologies that are used to broaden the attack surface are also used to automate cybersecurity detection and prevention.

Automation, on the other hand, must be employed strategically. There will be instances when automation identifies a threat, but the threat will not be severe enough to cause a manufacturing line to stop. The mechanisms must be in place to determine whether we can deal with the threat without shutting down production. For manufacturing executives, this includes making certain that their staff are:

- Using a cybersecurity platform paradigm, in which security teams may simply combine multiple technologies and have faster access to innovation.
- Moving to a Zero Trust architecture, in which only authorized users, using approved apps on authorized devices, are permitted access to the network, whether they are workers, partners, or anyone else in the supply chain.
- Automation, artificial intelligence, and machine learning are all being utilized to ensure that intelligence is incorporated at every stage of the production process.
- Making cybersecurity the organization's top priority and ensuring that it is taken into account anytime new technology, processes, or procedures are implemented or addressed.

The statement "The Path to Industry 4.0 and Society 5.0 Is Through Cybersecurity" is always resolute.

The Internet of Things is linking man-made things with people, and this is generating huge data by exchanging knowledge and information. AI-powered technology such as robotics and self-driving cars are helping to tackle social issues. Society 5.0 is Japan's vision for future, it is a society in which virtual space or cyber space and the physical space is interwoven to ensure economic progress, is balanced along with the solving of different social problems. However, in this Society 5.0, new security threats may emerge (Faruqee & Mühleisen, 2003).

Cyberattacks were first only a menace in cyberspace. But once physical space and virtual space are connected through IoT, consequences of cyber attacks would also be felt in real space. For example, A vulnerability that has been identified in an insulin pump, a piece of medical equipment that is used to inject insulin and monitor sugar levels in diabetic patients and if somehow this vulnerability is exploited, it may be likely used to give insulin incorrectly, resulting in a life-threatening condition. Traditionally, the term "security" was employed to safeguard the safety of virtual space, as opposed to "safety" in the physical space. However, in a period of the Society 5.0, we must consider the two together, as indicated in Figure 1.