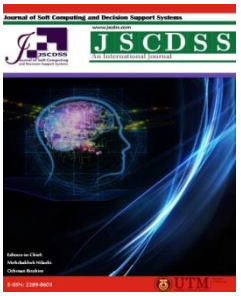
An International Journal
JSCDSS
http://www.jscdss.com
Vol.11 No.4 April 2024: 1-7
Article history:
Accepted 15 August 2024
Published online 15 August 2024

Journal of Soft Computing and Decision Support Systems



E-ISSN: 2289-8603

Evaluation of Security Pillars in the Industrial Internet of Things: A Fuzzy Logic Approach

Mehrbakhsh Nilashi [a,*]
[a] UCSI Graduate Business School, UCSI University, Cheras, Kuala Lumpur 56000, Malaysia

*** Corresponding author email address**: nilashidotnet@hotmail.com

Abstract
As the cyber and physical aspects of Internet of Things paradigms continue to advance, five pillars of information assurance (availability, integrity, non-repudiation, authentication, and confidentiality) have become insufficient to effectively reflect the IoT environment's overall security requirements. As a result, other security standards for cyber-physical Internet of Things environments are investigated and their importance is assessed in this study in the context of the Industrial Internet of Things. The fuzzy logic approach is adopted to measure the importance levels of these pillars. The results are provided and discussed.

Keywords: Industrial IoT, Security, Industry 4.0, Manufacturing, ANFIS

1. Methodology

The Internet of Things (IoT) facilitates smart cooperation between physical objects and their surrounding environments by integrating the physical and Internet-connected realms (Ahmadi et al., 2019; Asadi et al., 2022; Malina et al., 2016). The adoption and use of the IoT has changed the way industries work, communicate, and use data. Manufacturing has experienced fast change, and an industry that was once hesitant to advance is now digitizing at incredible speeds (Guo et al., 2021). The Fourth Industrial Revolution, often known as Industry 4.0, is a convergence of digital and physical technologies that allows for the creation of responsive, interconnected systems (Okano, 2017; Zhang and Chen, 2020). In order to make educated and timely decisions across a range of industries, from the supply chain to the smart factory, organizations are turning to artificial intelligence, robots, edge computing, and the cloud. Product quality and factory operational efficiency can be improved in real-time with solutions built for the Industrial Internet of Things (IIoT), which make use of linked sensors and edge devices (Schneider, 2017).

Typically, Internet of Things devices operate in a variety of situations to achieve a variety of goals. Their functioning, however, should be subjected to stringent cyber security requirements as well as physical security requirements (Makhdoom et al., 2018). The engagement of transdisciplinary aspects, networks, algorithms, and other factors contribute to the composite nature of the Internet of Things ecosystems. As a result, the attack surfaces of IoT-based systems are progressively expanded, and the work of meeting security requirements becomes more difficult. In order to meet the predicted IoT security need, a solution that takes into account all factors is required. Despite this, Internet of Things devices typically functions in a crowded and open setting. As a result, IoT-based systems are vulnerable to being physically accessed by intruders or attackers. IoT-based systems are often coupled with wireless networks, which present an opportunity for attackers/intruders to impersonate eavesdropping in order to extract sensitive information from the transmission. Because of the resource-constrained characteristic of the devices based on the Internet of Things, these devices are unable to handle complex security solutions (Chaabouni et al., 2019). Consequently, maintaining the privacy or security of systems based on IoT is a diverse and challenging challenge that has piqued the interest of researchers and practitioners in both the industrial and academic domains (Sadeeq et al., 2018; Sicari et al., 2015). When the primary goal of a system based on IoT technologies is to provide simple access to anybody, anywhere, and at any time,