# (Wang et al., 2020)

The data capture architecture of this study is described in Figure 4. Data are captured from physical space. The real-time operation data have been accessed through a PLC and displayed on the HMI. PLC is connected to HMI using CN1 cable. V-SFT is used to create the interface to display machine data on HMI. HMI displays the status of the machine, such as engine speed, pressure from the cutting plate, operating time, output, and input and output platform height. HMI also connects with the digital dashboard for real-time monitoring. The digital dashboard is created with J-Mobile. J-Mobile is a software used to create a platform that completely covers connectivity, device management, process management, and data visualisation for the lower levels of industrial IoT platform architecture. JMobile can support this study, given that the machine under investigation is only equipped with a low level of iIoT capability. The digital dashboard can display the status, OEE, order scheduling, and alarm functions of the machine. The digital dashboard receives data from HMI, whereas HMI receives data from PLC. For machines with high IoT levels, several studies used AutomationML, OPC UA, and MTConnect for network configuration. This study uses Ethernet way for network configuration, given that the conventional machine such as DCM has limited IoT levels. HMI supports the Ethernet method to exchange data with the digital dashboard. The communication protocol used to connect the digital dashboard and HMI is Modbus TCP/IP, which uses an Ethernet protocol to exchange data to satisfy the real-time and reliability requirement. Modbus TCP/IP is the second category of industrial networks (Lu et al. 2020). The digital dashboard is connected to the database that stores order data. A mutual communication exists between the database and the machine through the digital dashboard. The data stored in the company’s database can be accessed and displayed on the digital dashboard to support the operations of a machine. Machine’s data on the dashboard can also be retrieved by the digital dashboard and then stored in DB1 in real time. The proposed DT design framework is a typically ideal pattern of DT. However, owing to the security consideration, the machine is operated by the customer side with confidential receipts that are not allowed to be changed externally. Thus, the data access/modification from the digital dashboard to the machine is disabled in practice. This implementation on DCM becomes a type of digital shadow.

# (Khan et al., 2020)

## Communication protocols for IIoT

In this section, we devise a taxonomy demonstrating the working of various communication protocols of IIoT.

Meng et al. [18] have proposed a ZMQ messaging design model which represents a generic and flexible Machine-to-Machine (M2M) messaging mechanism between the machines for event and command notification and data sharing. The experimentation using a case study of Quality inspection microwave sensor of food manufacturing production concludes that the proposed ZMQ technique is promising tool to deal with machine connectivity, machine presence and discovery, and messaging to allow ubiquitous data access and data interaction for rich sensing IoT application. The proposed technique solves the complex structure and heterogeneity problems of IIoT applications and contributes to cross-platform capability that allows the implementation on various powerful computers and light-weight devices.

Yang et al. [19] have first proposed two types of time synchronization attacks in IIoT called Absolute Slot Number (ASN) attack and Timeslot Template (TT) attack and then two algorithms called Sec\_ASN algorithm and Threshold Filter (TOF) have been proposed to counter the proposed two attacks using IEEE802.15.4e-based IIoT protocol stack. When new nodes join the network, they can receive incorrect values of ASN, under ASN attack. On the other hand in TT attack the malicious node misguide the legitimate node for calculating the error clock offset. The Sec\_ASN is the combination of authentication and a method called 2s + 1. The authentication is achieved through two steps, first verifying the information about the sender and then checking the sent information for tampering during communication. For the method 2s + 1, one node is selected from neighboring nodes as time parent node for synchronizations. TOF algorithm is proposed for clock offset estimation using least squares method through the difference between normal node times and sending time of the node.

Qiu et al. [20] have proposed a robust time synchronization scheme known as R-Sync which eliminates the isolated nodes to makes all nodes synchronized and also reduces energy consumption on entire synchronization process. Two timers are adopted to pull isolated nodes to join the synchronized networks. One timer is for time synchronization using two-way message exchanges and another timer at the beginning of the synchronization process. The authors have also introduced a root node selection algorithm to balance energy consumption among sensor nodes and extend the lifetime of sensor networks. The proposed algorithm is compared with three existing time synchronization algorithms, Timing-sync Protocol for Sensor Networks (TPSN), Groupwise Pair selection Algorithm (GPA), and Spanning Tree-based Energy-efficient Time Synchronization (STETS) and through experimentation it is shown that the proposed R-Sync algorithms has lower energy consumption than GPA, TPSN and STETS algorithms, especially in densely connected and large scale networks.

Katsikeas et al. [21] studied the security implementation of MQTT (Message Queue Telemetry Transport) protocol using payload encryption (with AES, AES-CBC, AES-OCB) and link layer (with encryption with AES-CCM) in industrial domain. The authors evaluated and compared the secure and lightweight MQTT implementation using WSN testbed (Raspberry Pi) and through simulator. Two nodes are used during evaluation process, Publisher to emulate IIoT sensors and encrypt the data, and Subscriber to emulate IIoT actuators and decrypt the data. For comparison, latency, memory usage and energy consumption are considered. It is observed that MQTT implantation payload encryption (with AES, AES-CBC, AES-OCB) required more memory, energy and high latency as compare to MQTT implantation with link layer (with encryption with AES-CCM). However, if payload size is limiting factor, AES-CBC could be a better option.

Ferrari et al. [22] have investigated the latency of MQTT protocol for IIoT by observing the round trip time (RTT) through transferring data from the field to the Clouds and back. The authors have used embedded device IoT2040 from Siemens, energy saving Intel Quark x1020 (+secure boot), 1 GB RAM, 2 ethernet ports, 2xRS232/485 interfaces, battery backed RTC, Yocto Linux and industrial PC Intel i3-5000 with Windows 7 for the experimentation. The experimental works conclude that intercontinental roundtrip latency is less than 300ms, while local roundtrip latency is achieved at less than 50ms. The roundtrip delay is caused by the free Clouds used, internet connection, and the used hardware. However, implementation of filter reduces the values effectively.

Kiran et al. [23] have proposed a novel Markov chain based analytical/theoretical model to analyze the performance of unslotted Prioritized Contention Access (PCA) and Carrier-sense Multiple Access with Collision Avoidance (CSMA/CA) in nonbeacon-enabled PAN and slotted PCA and CSMA/CA in beacon enabled Personal Area Network (PAN). The reliability and the performance of the proposed model with less than 5% error is validated using Monte Carlo simulation and real-time test bed. The achieved results of slotted PCA claim that the reduction of 63.3% and 97% in delay and power consumption respectively compared with the slotted CSMA/CA, whereas unslotted PCA achieves reduction of 53.3% and 96% for delay and power consumption, respectively compared with unslotted CSMA/CA without significant loss of reliability.

# (Zhou et al., 2022)

# References

Khan, W.Z. *et al.* (2020) ‘Industrial internet of things: Recent advances, enabling technologies and open challenges’, *Computers &amp; Electrical Engineering*, 81, p. 106522. doi:10.1016/j.compeleceng.2019.106522.

Zhou, Y. *et al.* (2022) ‘A digital twin-based Operation Status Monitoring System for port cranes’, *Sensors*, 22(9), p. 3216. doi:10.3390/s22093216.