INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 15, Issue 8, (2025) E-ISSN: 2222-6990

Internet of Things Competencies for Mechanical Engineers

Nur Shahirah Mohamed Nasir, Muhammad Sukri Saud, Nurul Aini Mohd Ahyan

Faculty of Educational Sciences and Technology, Universiti Teknologi Malaysia, 81310
Johor Bahru, Johor, Malaysia

Email: nurshahirah1997@graduate.utm.my, p-sukri@utm.my, nurul.aini@utm.my

DOI Link: http://dx.doi.org/10.6007/IJARBSS/v15-i8/26077

Published Date: 03 August 2025

Abstract

The Internet of Things (IoT) is changing the way mechanical engineers work by introducing smart devices, real-time data, and automation into industrial systems. Therefore, engineers need to acquire new skills to remain relevant in this modern environment. This article identifies seven key competencies that mechanical engineers must develop, including IoT system architecture, integration and sensor calibration, communications protocols, embedded systems, data analysis for predictive maintenance, cybersecurity, and industry automation. Each area is discussed in terms of how it supports real-world applications such as improving machine performance, predicting damage, and enabling automatic control. This study also emphasized the importance of combining technical knowledge with analytical thinking to solve emerging industrial challenges. By strengthening these interdisciplinary skills, engineers can better adapt to connected environments and optimize system-level outcomes. To support industry educators, institutions, and leaders, a competency-based framework is proposed to guide professional training, curriculum design, and workforce development to ensure alignment with the demands of Industry 4.0.

Keyword: Internet of Things (IoT), Mechanical Engineering, TVET, Industry 4.0, Industrial Automation

Introduction

The Internet of Things (IoT) has become a key driver of transformation across various industrial sectors, including mechanical engineering. By enabling seamless connectivity between devices, systems, and users, IoT supports smarter decision-making, real-time monitoring, and automation (Gubbi et al., 2013). In the field of mechanical engineering, this technology enhances efficiency, facilitates predictive maintenance, and optimizes operations by continuously collecting and analyzing performance data (Miorandi et al., 2012). For example, IoT can reduce unplanned downtime by detecting early signs of mechanical wear, improve energy usage through sensor feedback, and support remote system monitoring (Lee et al., 2015).

With the widespread adoption of Industry 4.0 technologies, industries are increasingly seeking mechanical engineers who are not only technically proficient but also capable of integrating digital systems. This highlights a growing demand for engineers equipped with specific IoT competencies. However, there is still limited clarity on which skills are most essential and how they can be systematically developed through education and training.

As more industries adopt IoT technology, the need for mechanical engineers with such skills is increasing (Xu et al., 2014). Engineers now need to understand how the IoT system works, from sensors and communication protocols to data analysis and system integration (Zhou et al., 2015). These skills are important for managing and improving intelligent machines and connected environments.

This paper is particularly relevant for engineering educators, curriculum developers, and industry practitioners who are preparing students and professionals for a rapidly evolving industrial environment. By identifying the core IoT competencies for mechanical engineers, this research addresses a significant skills gap that could impact workforce readiness and industrial competitiveness. The insights gained from this study will help align engineering education with the practical demands of Industry 4.0, enabling engineers to contribute more effectively to smart manufacturing and sustainable innovation.

Therefore, this paper aims to examine the key IoT competencies required by mechanical engineers. It also explores how these skills are applied in areas such as automation, manufacturing, and predictive maintenance. By providing a structured competency framework, this study supports the development of future-ready engineers who can navigate and lead in IoT-integrated industrial settings.

Methodology

This study employs structured literature reviews to examine the primary competencies of the Internet of Things (IoT) essential in mechanical engineering. The goal is to develop a clear framework that reflects the knowledge and technical skills needed in today's IoT-based industry settings.

This study focuses on academic articles, technical papers, and industry guidelines published between 2012 and 2024. Sources are collected from Google Scholar. The keywords used in the search include "IoT in mechanical engineering," "forecast maintenance," "sensor integration," and "smart milling." Of the more than 2,000 results, the list was narrowed down to 21 high-quality sources based on relevance and credibility.

To ensure that the study remains focused on mechanical engineering, only sources that cover the integration of IoT technology in mechanical systems are included. Paper that concentrates solely on electrical, civil, or general computer engineering is excluded unless they have a strong link to mechanical applications.

The selected articles have been examined to identify repeat themes and skill fields. These are then grouped into seven core competency domains: IoT architecture, sensor integration, communications protocols, sensing systems, data analysis for forecasting and maintenance, cybersecurity, and automation.

A qualitative synthesis approach is employed to analyze the information and elucidate the relationship between competence and industry needs. This method helps build a structured framework that can guide curriculum development, engineering training programs, and workforce preparation for Industry 4.0.

Objectives

This study aims to identify and explain the key IoT competencies needed by mechanical engineers to succeed in the modern industry environment. By reviewing the latest research and real-world practices, this study sets out:

1. Determine the key areas of IoT skills related to mechanical engineering. These include system architecture, sensor integration, communication protocols, embedded systems, data analytics, cybersecurity, and automation.

2. Shows how these skills are used in the real industrial environment.

3. Suggest a practical competency framework that educators, coaches, and industry leaders can use for engineers to work in an IoT-driven environment in line with Industry 4.0.

Findings and Discussion

Findings

Understanding of IoT Architecture

For mechanical engineers working with IoT systems, a strong understanding of IoT architecture is essential. This architecture comprises a network of components, including sensors, actuators, communication protocols, and processing units, that collaborate to monitor and control machines in real-time (Gubbi et al., 2013).

The sensor acts as a significant interface with the physical world. They collect data such as temperature, vibration, or pressure. For example, the temperature sensor on the motor can detect when it is too hot, while the vibration sensor may take an initial sign of mechanical wear (Miorandi et al., 2012). The driver responds to this data, for example, by adjusting the robot arm or controlling the machine's speed (Lee et al., 2015). These interactions depend on communication protocols such as Wi-Fi, Bluetooth, Zigbee, or LoRa, which are selected based on factors such as range, speed, and power consumption (Khan et al., 2012). A sensor system or edge device typically processes the data collected and often sends it to the cloud for in-depth analysis, facilitating easy decision-making (Xu et al., 2014).

Engineers who have a clear understanding of this architecture can design more efficient systems that support automation and real-time monitoring. For example, in a smart factory, engineers must ensure that sensors, movers, and controllers work well together (Zhou et al., 2015). This enables the system to detect damage in advance, trigger an automatic response, and reduce damaged or stopped time (Boyes et al., 2018). It also helps engineers solve problems more effectively by identifying which components are performing less well in systems (Compare et al., 2019).

To succeed in this field, engineers need some technical skills. These include designing integrated systems, selecting appropriate communications technologies such as MQTT or BLE, and analyzing data to make informed decisions. Solving problems and optimizing performance are also essential skills, especially when working with complex machinery or heritage systems.

A good example is the use of IoT in predictive maintenance. Sensors, processed by microprocessors, collect data on vibration, temperature, and pressure, and send it to the cloud. If abnormal readings appear, such as irregular vibrations, warnings are triggered, allowing the maintenance team to act before damage occurs (Khan et al., 2012).

Data Acquisition and Sensor Integration

One of the most important skills for mechanical engineers in the IoT environment is the ability to select, install, and calibrate sensors. These sensors measure physical factors such as temperature, pressure, vibration, or flow rate, which are the primary data for monitoring and optimizing mechanical systems (Miorandi et al., 2012).

Engineers must understand how various types of sensors function and when to utilize them. For example, thermocouple and RTD help measure temperature, while piezoelectric sensors are often used to detect vibrations in spinning/rotating machinery (Lee et al., 2015). Installing sensors correctly is just as important as choosing the right type (Xu et al., 2014). Calibration is also important to ensure that sensors provide reliable measurements, especially in variable environments (Zhou et al., 2015).

With well-integrated sensors, engineers can monitor machines in real time. This helps them detect an unusual pattern and take action before the problem becomes serious (Khan et al., 2012). An everyday use case is predictive maintenance, where the vibration or temperature data of the motor is analyzed to detect the initial signs of failure. This approach reduces the time and cost of repair (Boyes et al., 2018). The sensors also help improve their overall performance by providing engineers with feedback that they can use to refine operations. For example, in heat exchangers, temperature and pressure sensors help maintain efficiency by maintaining the system in optimal condition (Compare et al., 2019; Gubbi et al., 2013)

To work effectively with sensors, engineers need a combination of technical knowledge and practical skills. They need to understand the principles of the various sensors, how to integrate them into the mechanical system, and how to ensure accuracy through proper calibration and maintenance. Equally importantly, they must be able to interpret the data and use it to support automation, performance adjustment, and error detection.

An example of a real-world application is the use of sensors in the HVAC system. Temperature and humidity sensors monitor air quality and energy consumption. When performance decreases, data helps engineers diagnose and correct issues quickly (Zhou et al., 2015). In manufacturing, a vibration sensor mounted on the motor or pump can detect the initial signs of wear. By acting on this information, engineers can schedule maintenance before severe damage occurs, extend the equipment's life, and avoid unexpected shutdowns (Khan et al., 2012).

Connectivity and Communication Protocols

For the IoT system to function effectively, mechanical engineers need to understand how the device communicates with other devices. This involves the proper selection and use of the communication protocol to ensure that data flows smoothly between sensors, controllers, and cloud platforms (Zanella et al., 2014).

Different protocols have different purposes. For close and low-power needs, technologies such as Zigbee or Bluetooth are often used (Gomez et al., 2012; Xiao et al., 2018). Instead, Wi-Fi offers faster data transfer, making it ideal for real-time monitoring and diagnostics (Al-Fuqaha et al., 2015). Lora is ideal for delivering a small amount of data remotely, especially in an isolated environment (Sundaram et al., 2020). Cellular networks, such as 4G and 5G, are beneficial when a machine requires continuous connectivity across a large area, as in mobile or field-based applications (Palattella et al., 2016).

Choosing the proper protocol depends on the situation. For example, in factories with numerous machines, engineers may utilize LoRa or Wi-Fi to ensure everything is connected. In a small network of sensors, Zigbee can be a better option as it uses less power (Zanella et al., 2014). In battery-powered devices, such as wearable tools or mobile monitoring tools, low-energy options like Bluetooth are more efficient (Gomez et al., 2012). In remote monitoring scenarios, such as offshore wind farms, cellular or LoRa networks ensure the continuous delivery of sensor data to central systems, enabling predictive maintenance and reducing system downtime (Al-Fuqaha et al., 2015) when fast data processing is crucial, as in video-based monitoring or robotic systems, Wi-Fi or 5G is often the solution of choice (Palattella et al., 2016).

To manage this technology well, engineers must develop some key skills. They need to understand the strengths and limitations of each protocol, be able to integrate the communication module into the mechanical system, and know how to minimize issues such as harassment or power drain gaps. Engineers also require a basic understanding of network design to ensure the system remains safe, scalable, and reliable.

For example, in a smart factory, temperature and vibration sensors may connect to the local gate using Zigbee, and the route can utilize Wi-Fi to transmit data to the cloud dashboard. In agriculture, soil sensors may utilize LoRa to transmit moisture readings from remote fields to base stations. These preparations underscore the significance of communication protocols in ensuring that machines and systems communicate effectively with one another (Sundaram et al., 2020; Xiao et al., 2018).

Embedded Systems and Microcontrollers

In IoT applications, mechanical engineers must understand how the embedded system and the microprocessor work. The system acts as a "brain" for smart devices, enabling the machine to respond to real-time sensor input and perform automatic tasks (Gubbi et al., 2013). Typically, an embedded system comprises a microprocessor, memory, input/output interfaces, and control logic that connect everything.

The microprocessor plays a key role by reading sensor data, controlling the driver, and handling communication between devices. Platforms such as Arduino are widely used for fast prototyping due to their simplicity and accessibility (Soori et al., 2023), while Raspberry Pi offers more power for complex tasks, such as image processing and local data analysis (Compare et al., 2019). Engineers also rely on microprocessors such as ESP32, which comes with Wi-Fi and Bluetooth built-in, making it ideal for wireless IoT industry applications (Al-Fuqaha et al., 2015).

The system appears in many real-world scenarios. For example, industrial robots may use embedded logic to adjust their movement based on sensor feedback. In the HVAC system, the temperature sensor sends data to a microprocessor, which determines whether to activate the fan or heater. This thoughtful response improves energy efficiency and reduces the need for manual control (Khan et al., 2012; Xu et al., 2014).

Engineers need strong technical skills to work with this system. They must know how to choose and connect sensors and actuators. Microprogrammers use languages such as C or Python to ensure that the system responds quickly and accurately. Understanding how to connect this device to the network using Wi-Fi, Bluetooth, or LoRa is also important.

The embedded system also supports remote monitoring and forecast maintenance. For example, microprocessors can collect temperature readings from industrial machinery and transmit the data to a cloud server via Wi-Fi. There, machine learning models can analyze data and alert engineers to situations that appear to be abnormal (Boyes et al., 2018). Thanks to their low cost and flexibility, platforms such as Arduino and Raspberry Pi are also helpful for prototypes and rapid testing before transitioning to large-scale use (Sundaram et al., 2020).

Data Analysis and Predictive Maintenance

In today's related industrial environment, mechanical engineers are expected to use data analysis to support predictive maintenance. This approach involves analyzing real-time data from sensors, such as temperature, vibration, and pressure, to monitor the equipment's health and anticipate potential tool failures (Khan et al., 2017). Moving from a reactive or fixed table, engineers can now make decision-driven decisions that reduce stopping time and improve machine performance.

To effectively carry out prediction maintenance, engineers need to be familiar with the tools and software used for data analysis. These include Python, R, and MATLAB for statistical processing, as well as similar platforms like Tableau for data visualization. Some engineers also utilize machine learning libraries, such as TensorFlow, to develop models that can detect patterns in equipment behavior and predict failures before they occur (Kanawaday & Sane, 2017).

Understanding prediction modeling is another important skill. Engineers employ techniques such as regression analysis, decision trees, or neural networks to identify early warning signs of damage (Al-Fuqaha et al., 2015). However, before the data is analyzed, it must be cleaned and prepared through pre-processing tasks, such as formatting, normalizing, or removing noise (Xu et al., 2014). This ensures that the decision is accurate and can be taken.

The actual value of predictive maintenance lies in its ability to extend the equipment's life and reduce costs. For example, the vibration sensor on the pump may detect an abnormal signal that indicates worn bearings. With the initial warning, the maintenance team can intervene before the pump fails (Khan et al., 2017). Similarly, the gradual change in temperature flow from the furnace may indicate a fundamental issue that requires attention before it causes damage (Zhou et al., 2015).

Engineers must also be able to design effective maintenance strategies. Instead of relying on fixed service intervals, they use sensor data to guide interventions based on actual equipment conditions (Boyes et al., 2018). This situation, based on this condition, is more efficient and reduces unnecessary services.

In real-world applications, this is evident in CNC machines equipped with sensors that monitor vibration and temperature. Data from these sensors is processed through cloud-based systems using predictive models. If signs of overheating or malfunction are detected, an automatic alert is sent so the engineer can take the necessary precautions. This ensures that the machine operates more efficiently, reduces repair costs, and increases productivity (Al-Fuqaha et al., 2015). The HVAC system provides another example, where temperature and pressure data help detect leaks or inefficiencies. Prediction algorithms then guide timely repairs, increasing system reliability and energy consumption (Xu et al., 2014).

Security and Privacy in IoT

As the IoT system becomes more common in mechanical engineering, engineers must be equipped to address serious concerns about safety and privacy. Connecting machines and devices increases the risk of cyber-attacks, data violations, and unauthorized access. Mechanical engineers must understand how to design a safe system that protects sensitive data and ensures the safe operation of industrial equipment (Sicari et al., 2015).

A solid foundation in IoT security begins by understanding how to keep data safe. Encryption plays a crucial role, with technologies such as AES and TLS helping to protect data during storage and transmission (Zhou et al., 2015). Verification methods are also important. Using techniques such as multi-factor authentication, device-specific tokens, or biometrics ensures that only authorized users and devices are allowed to access the system (Al-Fuqaha et al., 2015).

Engineers also need to implement access control strategies. Role-based access control (RBAC), for example, limits the individuals who can view or modify system components, adding a layer of protection (Boyes et al., 2018). To make data exchange safer, engineers can rely on protocols such as SSL/TLS, VPN, or MQTT. This tool facilitates encrypted communication between devices and servers (Khan et al., 2012). Invasion detection systems (IDS) and firewalls are just as important, as they monitor traffic and identify suspicious activities (Xu et al., 2014).

Updating the device is another important part of IoT security. Engineers should utilize software updates, delivered via over-the-air (OTA) updates, ideally, to mitigate weaknesses and ensure the system's resilience to new threats (Patil et al., 2024).

Practically, this step is crucial in settings such as an automated factory. For example, if the robot's arm is not adequately secured, cyber-attacks can alter its behavior and cause damage. Encrypted control and instructions help prevent this (Sicari et al., 2015). Similarly, industry IoT devices continuously submit data on machine performance, inventory, or quality control. If this information is intercepted or altered, it may interfere with the operation. Encryption from end to end ensures that data remains personal and unchanged (Zhou et al., 2015). Similarly, IoT-enabled robotic systems must be protected from unauthorized reprogramming through robust verification controls to prevent costly operational disruptions (Bhatt et al., 2021).

Engineers must also consider the security of the cloud platform, where most IoT data is processed and stored. Using secure firewalls, VPNs, and cloud-level encryption is important. In some cases, naming data helps protect consumer privacy while still allowing functional analysis (Al-Fuqaha et al., 2015). Engineers must also comply with regulations such as ISO/IEC 27001, NIST, and GDPR cybersecurity frameworks, especially when handling personal or operating data (Xu et al., 2014).

To accomplish all this, engineers require specific competencies. These include utilizing security protocols such as TLS, VPN, and AES encryption, managing device-level security, detecting and preventing threats, and adhering to privacy rules. Together, these skills ensure that the connected system remains safe, reliable, and in compliance with industry standards.

For example, in smart factories, sensors, machines, and robots are all linked through safe channels. TLS encryption protects the data they send, while RBAC ensures that only authorized staff can modify the system settings. Frequent OTA updates help ensure that each device is protected from new cyber threats. This practice fosters a secure environment that enables automation and connectivity to thrive without compromising security or data integrity.

System Integration and Automation

In the modern industrial environment, mechanical engineers must be proficient in integrating systems and automating IoT technology. This means that engineers must be able to integrate sensors, drivers, controllers, and communication networks into a real-life system that can operate in real-time (Ashima et al., 2021). With proper integration, traditional machines can be an innovative system that automatically adjusts its movement based on real-time data.

System integration begins with designing how different devices interact with each other. Engineers need to configure innovative components, such as sensors and microprocessors, across various machines, including robot arms, CNC machines, and conveyors (Boyes et al., 2018). To enable these devices to communicate effectively, they must use industry protocols such as Modbus, OPC UA, or CAN Bus (Khan et al., 2012). Engineers also handle IoT device setups such as entrances and edge processors, which collect and transmit data to the control system (Zhou et al., 2015).

Another core skill is the programming automation system. Engineers often utilize tools such as Programmable Logic Controllers (PLCs), SCADA, or Distributed Control Systems (DCS) to automate machine actions based on sensor feedback (Xu et al., 2014). Understanding data communication is also crucial to ensure the system remains constantly connected, utilizing networks such as Wi-Fi, Zigbee, or LoRa (Ashima et al., 2021).

In real-world applications, this type of integration dominates everything from an automatic installation line to an intelligent energy system. For example, sensors mounted on robot arms or conveyors can detect speed, wrong, or vibration. Data is processed immediately, and the system can automatically adjust to avoid errors or interruptions (Ashima et al., 2021). Prediction maintenance is also easier, as sensors detect early warning signs, and automation protocols trigger warnings or moisture alerts before damage occurs (Al-Fuqaha et al., 2015).

Intelligent robots are another example. In car manufacturing, robot arms utilize real-time sensor feedback to refine their alignment and position, thereby improving accuracy and reducing defects (Kanawaday & Sane, 2017). Outside of performance, IoT automation also supports sustainability. For example, the HVAC system or lighting system in a factory uses occupancy and environmental sensors to reduce energy consumption in uninhabited areas (Zhou et al., 2015). Machines can even turn off or reduce power automatically during peak hours to reduce costs.

Flexible production is another significant benefit. IoT integration enables machines, such as 3D printers or CNC tools, to reconfigure themselves based on updated data, allowing for custom manufacturing with minimal human input (Ashima et al., 2021).

To make an expert engineer in this field, engineers must understand how to coordinate all elements in connected systems, from sensors and controllers to networks and automation tools. They should also be familiar with the programming of controls, sensors, communication protocols, and interface tools, such as HMI (human-machine interface), that enable system visualization and monitoring.

Examples of good integration include the smart factory, where machines report temperature, vibration, and production speed. If the sensor detects excessive heat, the system can automatically activate the cooling system or slow down the machine. RFID tags and barcode scanners can also track inventory in real-time, triggering stock alerts or adjusting production flows according to requirements (Ashima et al., 2021). This solution reduces human error, increases productivity, and enables more intelligent and adaptable operations.

Discussion

In today's industry, this competency corresponds to what employers expect. As the smart factory, forecasting system, and digital twins became more prevalent, mechanical engineers were no longer concentrated solely on mechanical design (Compare et al., 2019; Lee et al., 2015). They are expected to encode microprocessors, understand sensor data, and protect connected systems. This shift means that engineers must be prepared to bridge the gap between the physical and digital worlds, especially in environments that demand quick decisions based on real-time views (Al-Fuqaha et al., 2015; Xu et al., 2014).

This transition has significant implications for engineering education and professional development. The traditional mechanical engineering curriculum, which often focuses on manual systems and theoretical concepts, may not be enough. There is a growing need to inculcate inter-disciplinary learning that combines elements of computer science, electronics, and data analysis (Kanawaday & Sane, 2017; Soori et al., 2023). Practical experience with platforms such as Arduino, Raspberry Pi, and ESP32, combined with exposure to cloud platforms and safety protocols, can better provide students with the challenges of Industry 4.0 (Ashima et al., 2021; Sundaram et al., 2020).

However, implementing these changes comes with challenges. Many institutions face limited access to modern IoT infrastructure, which restricts direct learning opportunities (Bhatt et al., 2021). The rapid evolution of technology also puts pressure on curriculum developers in line with industry needs. In addition, a growing skill gap exists between traditionally trained engineers and those experienced in digital systems, underscoring the need for continuous learning and skill improvement (Patil et al., 2024; Zhou et al., 2015).

Despite these obstacles, the opportunity is enormous. IoT competence enables the creation of autonomous machines, adaptive manufacturing systems, and energy efficiency solutions that respond to real-time conditions. Engineers with skills in system integration, analytics, and automation are well-positioned to lead innovation in robotics, innovative infrastructure, and sustainable production (Khan et al., 2017; Miorandi et al., 2012).

The competency also encourages system thinking approaches, where engineers understand how hardware, software, and data interact to improve performance, reduce costs, and improve reliability (Compare et al., 2019; Sicari et al., 2015). This holistic perspective is increasing as the industry moves towards smart operations.

In conclusion, IoT is redefining the role of mechanical engineers. The mastery of a technical field is no longer enough. Engineers must be able to connect systems, interpret data, and ensure safe operations across complex networks to maintain efficient and reliable systems. The framework developed in this study provides the basis for training mechanical engineers who can adjust, possess digital literacy, and are ready to thrive in the 4.0 industry. Based on the findings, Figure 1 shows the IoT competency framework for mechanical engineers.

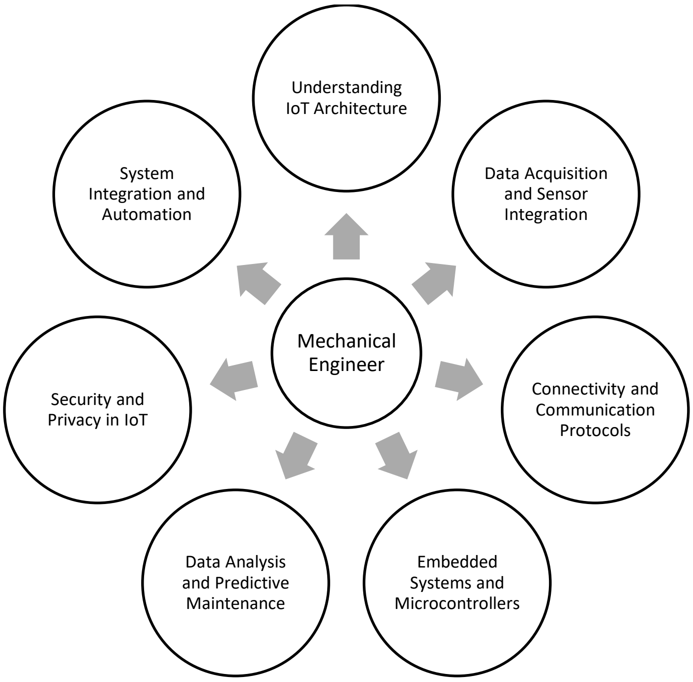
Understanding IoT Architecture
Data Acquisition and Sensor Integration
Connectivity and Communication Protocols
Embedded Systems and Microcontrollers
Data Analysis and Predictive Maintenance
Security and Privacy in IoT
System Integration and Automation
Mechanical Engineer

Figure 1 IoT Competency Framework for Mechanical Engineers

Conclusion

The integration of IoT technology into mechanical engineering is no longer an option; the industry needs to strive for enhanced automation, reliability, and efficiency. As the transition to Industry 4.0 is rapid, mechanical engineers must be equipped with a range of competencies that extend beyond traditional technical skills. These include the ability to design IoT architecture, integrate and calibrate sensors, set system programs, select appropriate communications protocols, and analyze data for predictive maintenance.

One of the most valuable contributions of IoT in this field is the step towards predictive maintenance. By analyzing data from sensors, such as temperature, pressure, and vibration, engineers can identify potential issues and take action before they fail. This not only reduces stoppages but also extends the life of the machinery and lowers maintenance costs.

Automation and system integration also change the way engineers work. Smart sensors, microprocessors, and cloud platforms now allow real-time control and adjustment systems that respond to changes in the situation with little human intervention. This opens up opportunities for scaling operations, energy efficiency in manufacturing, and more.

However, as more devices are connected, security and privacy challenges become more urgent. Mechanical engineers must understand how to perform decoding, manage verification, and control access to keep the system safe and resilient. Compliance with standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework is crucial for protecting sensitive data and maintaining operational trust. The evolution of continuous IoT technology means engineers must continue to learn to stay competitive. Those who are skilled in data analysis, automation, and safe system design will be more prepared to contribute to smart factories, autonomous machines, and sustainable industry solutions. This competency supports innovation and adaptability, which are important features as the industry transitions to a fully connected ecosystem.

Ultimately, this study highlights the need for a comprehensive competency framework that informs education, training, and professional development in IoT-based mechanical engineering. By accepting this competency, engineers can lead transformations towards an innovative, data-driven industrial environment and be more prepared for the future.

Acknowledgement
The author would like to express his deepest gratitude to Universiti Teknologi Malaysia and this study was supported by the Nexus Young Researcher Grant 2023 – UTMFR [PY/2023/01370].

References

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347-2376.

Ashima, R., Haleem, A., Bahl, S., Javaid, M., Mahla, S. K., & Singh, S. (2021). Automation and manufacturing of smart materials in Additive Manufacturing technologies using Internet of Things towards the adoption of Industry 4.0. *Materials Today: Proceedings, 45*, 5081-5088.

Bhatt, S., Pham, T. K., Gupta, M., Benson, J., Park, J., & Sandhu, R. (2021). Attribute-based access control for AWS internet of things and secure industries of the future. *IEEE Access, 9*, 107200-107223.

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry, 101*, 1-12.

Compare, M., Baraldi, P., & Zio, E. (2019). Challenges to IoT-enabled predictive maintenance for industry 4.0. *Ieee Internet of Things Journal, 7*(5), 4585-4597.

Gomez, C., Oller, J., & Paradells, J. (2012). Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors, 12*(9), 11734-11753.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645-1660.

Kanawaday, A., & Sane, A. (2017). *Machine learning for predictive maintenance of industrial machines using IoT sensor data.* Paper presented at the 2017 8th IEEE international conference on software engineering and service science (ICSESS).

Khan, M., Wu, X., Xu, X., & Dou, W. (2017). *Big data challenges and opportunities in the hype of Industry 4.0.* Paper presented at the 2017 IEEE International Conference on Communications (ICC).

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). *Future internet: the internet of things architecture, possible applications and key challenges.* Paper presented at the 2012 10th international conference on frontiers of information technology.

Lee, J., Bagheri, B., & Kao, H.-A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing letters, 3*, 18-23.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497-1516. doi:https://doi.org/10.1016/j.adhoc.2012.02.016

Palattella, M. R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T., & Ladid, L. (2016). Internet of things in the 5G era: Enablers, architecture, and business models. *IEEE journal on selected areas in communications, 34*(3), 510-527.

Patil, R. Y., Patil, Y. H., Manna, A., & Ranjanikar, M. (2024). Enhancing the security of firmware over-the-air updates in automotive cyber-physical system. In *Cyber Physical System 2.0* (pp. 282-301): CRC Press.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146-164.

Soori, M., Arezoo, B., & Dastres, R. (2023). Internet of things for smart factories in industry 4.0, a review. *Internet of Things and Cyber-Physical Systems, 3*, 192-204. doi:https://doi.org/10.1016/j.iotcps.2023.04.006

Sundaram, J. P. S., Du, W., & Zhao, Z. (2020). A Survey on LoRa Networking: Research Problems, Current Solutions, and Open Issues. *IEEE Communications Surveys & Tutorials, 22*(1), 371-388. doi:10.1109/COMST.2019.2949598

Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? *IEEE Signal Processing Magazine, 35*(5), 41-49.

Xu, L. D., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics, 10*(4), 2233-2243.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *Ieee Internet of Things Journal, 1*(1), 22-32.

Zhou, K., Liu, T., & Zhou, L. (2015). *Industry 4.0: Towards future industrial opportunities and challenges.* Paper presented at the 2015 12th International conference on fuzzy systems and knowledge discovery (FSKD).