RESEARCH ARTICLE OPEN ACCESS

A Secure Digital Twin Framework for Autonomous Manufacturing in Smart Food Industries

Shajahan Basheer, Likitha N, Anusha A. Jerald Nirmal Kumar S
School of Computer Science and Engineering, Jain (Deemed-To-Be University) Bangalore, India
Bshajahan001@gmail.com, juug24btech19439@jainuniversity.ac.in, juug24btech23543@jainuniversity.ac.in, jerald@jainuniversity.ac.in.

Abstract:
The adoption of technologies like Cyber-Physical Systems (CPS) and Industrial Internet of Things (IIoT) in manufacturing has increased because of Industry 4.0. In food manufacturing Digital Twins combined with these technologies help keep virtual systems in sync, in real-time. The integration of technologies like CPS, IIoT, and Digital Twin makes the smart manufacturing efficient. This supports tasks like predicting when maintenance is needed and making decisions, which in turn boosts productivity and product quality. As quantum computers pose a threat we need to add Post-Quantum Cryptography to these frameworks to ensure they remain secure for a time. The food manufacturing industry can benefit a lot from these technologies. Digital Twins, Cyber-Physical Systems and Industrial Internet of Things technologies are increasingly being adopted in smart food manufacturing, yet face several critical deployment challenges. These interconnected systems are vulnerable to cyber-security threats including malware, ransomware and unauthorized intrusions that disrupt manufacturing operations and compromise product quality. Another important challenge is the lack of secure frameworks to enable trustworthy autonomous decision-making with security, reliability and continuity of the system. This paper covers the fundamentals of Digital Twin technology and its integration with Artificial Intelligence, Industrial Internet of Things, and Cyber-Physical Systems in smart food manufacturing. It explores the security vulnerabilities of autonomous systems enabled with Digital Twins. The chapter also covers secure architectural frameworks for Digital Twin technology and autonomous manufacturing processes. The chapter provides a comprehensive understanding of Digital Twin frameworks, identifies food safety and regulatory compliance considerations, and highlights security mechanisms for enhancing system resilience and autonomous decision-making. It also offers insights into future research directions for developing secure, post-quantum resilient, intelligent, and sustainable smart food manufacturing ecosystems.

Keywords: Digital Twin; Cyber-Physical Systems (CPS); Industrial Internet of Things(IIoT); Smart Food Manufacturing; Post-Quantum Cryptography (PQC); Autonomous Decision-Making; Cybersecurity.

I. INTRODUCTION

A. Background

Conventional food processing has relied heavily on manual labour, isolated mechanical design, and large generic production systems with little automation. The First Industrial Revolution brought about by water and steam power, then electricity with the Second, set assembly-line production in motion in the Third one that made food processing on a larger scale efficient. These traditional systems provided little connectivity, real-time monitoring and enabled reactive instead of proactive decision-making making it difficult to maximize production efficiencies, maintain consistent product quality and respond swiftly to changing market needs [2][8].

This is exactly where the Smart Manufacturing arises, a vision based on the collaboration of Industry 4.0 principles converging to transform food and beverage industry into an inter connected data-driven ecosystem. Smart manufacturing fuses together technologies (Internet of Things, Cyber-Physical Systems, Artificial Intelligence, cloud computing and advanced data analytics) that allow real-time monitoring; intelligent automation; predictive maintenance; and data-driven decision-making over the course of production. These features improve operating efficiency, product quality, traceability and resource utilization while boosting overall manufacturing resilience enabling the creation of secure, autonomous food production systems[9].

A Digital Twin (DT) is a dynamic virtual representation of a physical object, process, or system that is frequently updated with real-time data from its real-world counterpart. Based on the Sensor data and technologies like IoT, Artificial Intelligence (AI), and Advanced Analytics, a Digital Twin accurately reflects the operational state and behaviour of a physical twin in service [1][3]. This synchronization powers real-time condition monitoring, simulation, predictive analysis and performance enhancement so that engineers and organizations can test numerous operating scenarios, foresee equipment failures, refine maintenance strategies, and help decision making without disrupting or risking the physical system itself [16][19].

Inside the food industry, Digital Twins have been extraordinarily game-changing — capturing not only an individual asset but laying a foundation throughout complete production and supply chains. This capability offers manufacturers the ability to track their operations, simulate production scenarios, and optimize processes in real-time while increasing product quality and verifying traceability all while helping regulatory compliance and reducing food waste throughout the lifecycle of products [10][18].

With food manufacturing systems evolving towards greater interconnectivity and autonomy, securing them against attacks and making them resilient to failures is becoming a leading concern. By combining Industrial Internet of Things (IIoT) devices, cloud platforms and AI, these innovations are susceptible to new cybersecurity threats that can potentially disrupt production continuity, pollute data integrity and consumer safety.

For this reason, secure Digital Twin frameworks — based on autonomous decision-making, trustworthy communication and guaranteed (cyber-)security — are an essential building block for resilient, efficient and trustable smart food manufacturing systems.

B. Motivation

Digital transformation of manufacturing has had a huge positive impact on the efficiency, automation and operational intelligence in production. The food industry has it's own level of challenges, but these differ from general manufacturing. Ensuring product quality, safety and adherence to increasingly stringent regulatory standards cannot be accomplished without real-time monitoring and data-driven decision making throughout the production lifecycle to help minimize waste and maintain end-to-end traceability. Supply chains are becoming more complex, consumer expectations are evolving and the frequency of cyberattacks against connected industrial systems is increasing, all amplifying these demands [16].

Though existing Digital Twin frameworks have demonstrated significant promise for real-time monitoring, predictive maintenance and process optimization; most were designed for general manufacturing environments with limited focus on the unique operational demand of smart food industries [3][10]. The aforementioned gap underscores the requirement for integrated frameworks that assimilate Digital Twins with Artificial Intelligence (AI), Industrial Internet of Things (IIoT), advanced cybersecurity mechanisms, and secure communication technologies to empower resilient, intelligent, and trustworthy food manufacturing systems — frameworks fortifying operational efficiency whilst augmenting operability in terms of food safety, traceability, and manufacturing resilience [18].

C. *Role of Digital Twins*

The Digital Twins enable monitoring in real time by keeping an up-to-date relation between the actual manufacturing asset and its digital twin counterpart. Digital Twins use Internet of Things (IoT) sensors, Cyber-Physical Systems (CPS), and advanced communication technologies to provide complete visibility into equipment status, production processes, and environmental conditions. With such keen observation, manufacturers are able to monitor system performances and identify anomalies in their early stage — which helps the manufacturers make timely operational decisions and can ultimately improve the efficiency and reliability of production [1][3]. Predictive maintenance is another area where Digital Twins play an important role. They continually analyse real-time sensor data in conjunction with historical operational records, so manufacturers can predict impending equipment failure and assess the remaining useful life of critical components. Such maintenance strategies can then be validated in a virtual environment prior to implementation, resulting in reduced unplanned downtime, decreased maintenance expenses and improved overall reliability and availability of the manufacturing system [6][11]. Digital Twins also contribute to process optimization by creating a virtual environment in which production processes can be simulated under different operating conditions. This enables manufacturers to simulate different scenarios, identify bottlenecks, optimize resource utilization and tweak production scheduling without impacting live operations. This creates a feedback loop that improves operational efficiency, product quality, energy consumption and material waste throughout the entire manufacturing lifecycle the modern food industry [3]. In secure autonomous manufacturing, Digital Twins are intelligent decision support systems merging Artificial Intelligence (AI), Industrial Internet of Things (IIoT), cloud and edge computing and advanced cybersecurity technologies. The integration enables autonomous process control, secure data exchange, continuous risk assessment and fast reaction to changing operating conditions. They enhance food safety, traceability and regulatory compliance, in particular for smart food industries, and they help protect interconnected production systems from cyber threats. Therefore, Digital Twins have become an important enabling technology for secure, intelligent and autonomous manufacturing in the modern food industry [10][18].

II. LITERATURE SURVEY

Recent reviewed studies have established Cyber Physical Systems (CPS) and Digital Twin as the foundation of Industry 4.0 allowing predictive maintenance, simulation, real-time monitoring, and smart decision-making in manufacturing environments. Preliminary research focused on CPS architectures, data-driven manufacturing, smart factories and illustrate how technologies like Internet of Things (IoT), cloud computing, and sensors facilitate continuous communication with Physical components and digital systems. These technologies laid foundation for smart manufacturing, but limited implementation towards Digital Twin, security challenges and domain-specific applications. [1]-[9]

Future research introduced Digital Twin frameworks capable of sustaining constant coordination between physical and virtual counterparts. These models showed the enhancement in process optimisation, production planning, quality-control, and intelligent decision-making through integration of technologies like AI, ML, edge computing, cloud computing, and big data analytics. [10]-[22]

Most recent investigations explored adjustable Digital Twins models, data-driven manufacturing, Industry 5.0, blockchain enabled traceability, and viable smart manufacturing to improve flexibility and resilience of manufacturing and human-machine collaboration.

Nevertheless, most of the present systems focus only on general manufacturing environments in which that provide only limited assistance for food safety, and secure autonomous manufacturing systems. [23]-[35]

Overall, the literature indicates great strides in CPS, AI, IIoT, Digital Twin technologies for smart manufacturing. However, existing systems doesn't integrate AI-driven, Advanced cyber security, autonomous control, and real-time food monitoring frequently for Smart food manufacturing.

TABLE I. LITERATURE REVIEW

Reference	Focus Area	Technologies	Key contribution	Research gap
Tao & Zhang	Digital Twin manufacturing floor	Digital Twin, CPS, IoT	Real-time synchronisation	No specific food security
Tao et al.	Digital Twin and CPS	Digital Twin, CPS, AI	CPS-Digital Twin integration	No autonomous food manufacturing system
Biesinger et al.	Production planning	Digital Twin, CPS	Stronger scheduling ability	No cybersecurity
Ebnia et al.	Digital Twin framework	Digital twin, AI, IoT	Design to optimisation lifecycle	No food safety tools
Fuller et al.	Digital Twin review	Digital twin, AI, IoT	Empowering technologies and challenges	No domain specific framework.
Thelen et al.	Digital Twin modelling	Hybrid Digital Twin models	Modelling approaches	No secure architecture
Saeedi	Manufacturing Digital Twin	Digital Twin, CPS	Multi-level Digital Twin applications	Limited industrial validations
Zhong et al.	Intelligent manufacturing	CPS, IoT	Industry 4.0 foundation	Predates Digital Twin adoption
Cioffi et al.	AI in manufacturing	AI, ML	Autonomous manufacturing	No Digital Twin integration
Yao et al.	CPS Manufacturing	CPS, IoT	Smart manufacturing architecture	No DT-based framework
Zhang et al.	Redesignable Digital Twin	Digital Twin, CPS	Flexible Digital Twin architecture	No food manufacturing

III. Cyber Physical Systems and Digital Twin Technologies in Smart food manufacturing

The foundation of Industry 4.0 are Cyber Physical Systems and Digital Twin technologies, which facilitates connected, intelligent and autonomous manufacturing. CPS is the smart organisation which connects computers with real-world physical components like sensors, networks and feedback loops. CPS combines physical properties with sensors, embedded systems, communication networks, actuators and cloud platforms to enable data exchange, real-time monitoring, and automated control. CPS also facilitates predictive maintenance, process optimisation, quality monitoring, autonomous decision-making, flexibility, reliability, and enhance the speed of manufacturing through constant communication between physical processes and artificial intelligence. [1][2]

Digital Twin is constantly updated virtual representation of physical assets, process, or system based on the real-time data framework provided by the Cyber Physical Systems. Digital Twin maintains real-time synchronisation of the physical components by collecting continuous sensor data accumulated through CPS and IoT. Digital Twin allows simulation, process optimisation, predictive maintenance, and smart decision making with the integration of Artificial Intelligence, Edge computing, and advanced data analytics. [3][5]. The integration of CPS and Digital Twin technologies boost the product quality and food safety in smart food manufacturing. Continuous monitoring of vital parameters like humidity, temperature, pressure, pH, vibration allows early diagnosis of deviation of processes and equipment failures. Therefore, CPS and Digital Twins create an intelligent and secure smart food manufacturing system which enhances the speed of production, reduces wastage of food, streamline utilisation of resources and supports viable autonomous manufacturing. [16][22]

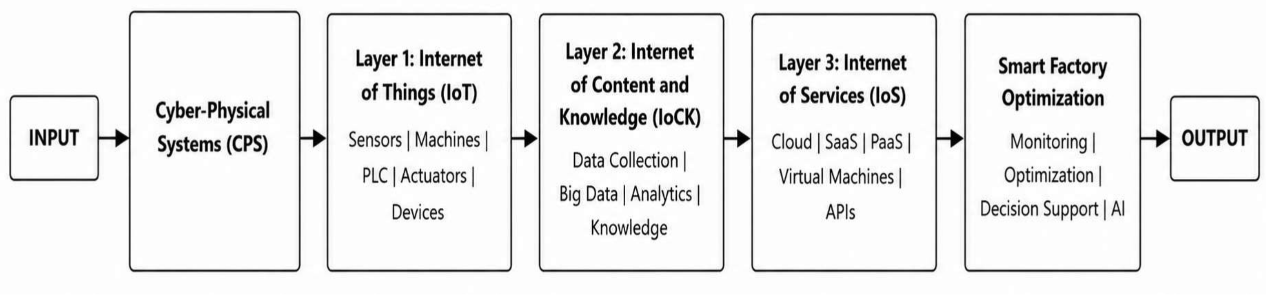

Fig. 1. CPS and Digital Twin

A. Working principle of CPS and Digital Twins

The working principle of Cyber-Physical Systems and Digital Twins are based on real-time replication between physical assets and their virtual components through continuous data exchange. First, embedded sensors and Industrial Internet of Things (IIoT) devices are implemented on manufacturing equipment, then gather operational parameters like temperature, humidity, pressure, energy consumption, vibration and current status of machines. Data transmission takes place securely through communication networks to cloud or edge computing, where it is processed and stored for further analysis. [10][11]

The continuous data processing updates Digital Twin, which allows to duplicate exactly the current state of the physical system. Data analysis is achieved using Artificial Intelligence (AI), Machine Learning (ML), and advanced analytics to detect anomalies, simulate operational scenarios and predict failures. Based on the analysis, Digital Twin generates automated control actions which can communicate with physical world finding closed-feedback loop for predictive maintenance. [1][3]

This simultaneous communication in Smart food manufacturing industries helps in constant process monitoring, contamination detection, food safety compliance, and smart resource management. The integration of technologies like CPS, IIoT, AI, Cloud computing, and Digital Twin allows autonomous decision-making, reduce production wastes, and improve the viability of smart food manufacturing systems. [11][18]

B. Challenges in implementing Cyber Physical Systems and Digital Twin

Irrespective of major advantages, implementation of Cyber Physical Systems (CPS) and Digital Twin also possess several technical limitations and operational challenges. Security remains as one of the major concern, as the sensors, networks, cloud platforms and digital twins are highly vulnerable to Cyber attacks, data breaches, and unauthorised access, and disrupts the systems which may compromise the product quality and consumer safety. [10][18]

Another big problem is getting devices, old manufacturing equipment and various communication protocols to work together. This makes it hard to integrate everything smoothly and share information in time. The Digital Twins are also very dependent on sensor data. If the data is not accurate or is missing it can make the predictions and automatic decisions less reliable. To use Cyber Physical Systems and Digital Twin technologies you need to spend a lot of money on sensors, computers, communication networks, skilled people and maintenance. This creates a financial hurdle, for small and medium sized food businesses [10][18]

The amount of real-time manufacturing data is getting bigger and bigger. This means we need storage that can handle a lot of information computers that can process it quickly and a way for systems to talk to each other fast. We have to make sure that the physical and virtual systems are always, in sync. To make this work we need to use communication protocols have strong cybersecurity to protect against threats manage data in a reliable way and find ways to implement these systems without spending too much money. This is really important if we want to have food manufacturing that is secure, intelligent and sustainable [18][23].

C. Working Principle

The basic concept of a Digital Twin is the ongoing synchronization of a physical entity and its virtual counterpart by means of real-time data exchange. This synchronization enables the virtual model to accurately reflect the operational state of the physical system, supporting continuous monitoring, simulation, analysis, and intelligent decision-making. The process involves a number of stages that are interconnected and, taken together, form a closed-loop feedback process.

Initially, the physical entity—such as manufacturing equipment, production lines, or food processing systems—continuously generates operational data through embedded sensors and Industrial Internet of Things (IIoT) devices. These sensors gather important parameters such as temperature, humidity, pressure, vibration, energy consumption, machine status, and product quality. The acquired data is sent over secure communication networks to cloud or edge computing platforms for storage and processing [10][11].

The collected data are then inputted to the virtual entity, where they are used to continually update the model of the Digital Twin. Artificial Intelligence (AI), Machine Learning (ML) and advanced data analytics analyse the incoming information to simulate the system behaviour, find operational patterns, detect anomalies and predict future performance. The virtual environment enables manufacturers to evaluate different operating scenarios, optimize production processes, and evaluate maintenance strategies without disrupting physical operations [1][3]. As a result of the analysis, the Digital Twin produces recommendations or automatic control actions to optimize the system performance. The decisions are transmitted to the physical entity via the communication network, allowing adaptive process control, predictive maintenance and autonomous decision-making. This two-way communication creates an ongoing feedback loop that allows the physical and virtual systems to be kept in synchronization throughout the manufacturing process.

The principle of operation is applied in smart food industries for continuous monitoring of the production process, early detection of equipment failures, optimization of manufacturing parameters, and maintenance of product quality and food safety standards. Digital Twins integrate Cyber-Physical Systems (CPS), the IIoT, AI, cloud computing, and secure communication technologies, providing a reliable platform for intelligent, secure, and autonomous manufacturing. This in turn increases the interaction between the physical and virtual environments, leading to operational efficiency, lower production costs, better resource utilization and resilient, sustainable food manufacturing systems[11][18].

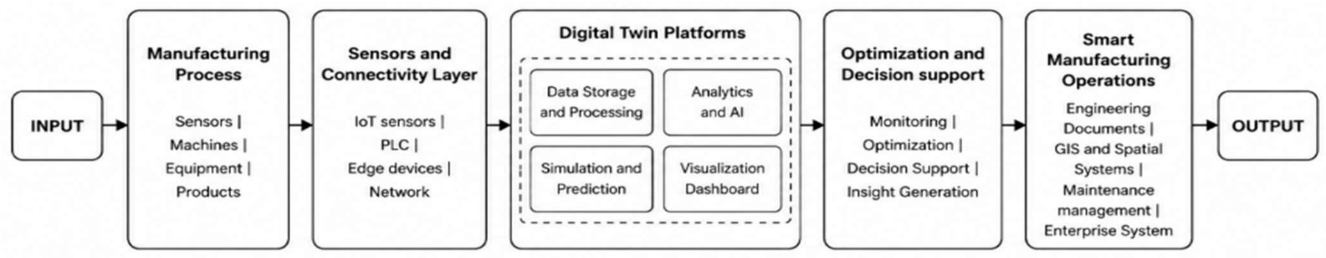

Fig 02: Digital Twin Platform

IV. AI-ENABLED DIGITAL TWIN

A. AI in Manufacturing

Artificial Intelligence (AI) is a disruptive technology for modern manufacturing, which enables intelligent automation, data-driven decision-making and autonomous process optimization. Unlike traditional manufacturing systems that depend heavily on pre-defined rules and manual intervention, AI-powered systems can learn continuously from operational data, discover hidden patterns, and make informed decisions with minimal human involvement. AI has greatly improved production efficiency, product quality, resource utilization and operational flexibility in manufacturing environments, and therefore has become a fundamental technology of Industry 4.0 [2][6].

In smart manufacturing, AI is integrated with enabling technologies such as the Industrial Internet of Things (IIoT), Cyber-Physical Systems (CPS), cloud computing, edge computing, and Digital Twins to establish intelligent, interconnected production settings.

Sensors implemented across manufacturing systems constantly generate large volumes of functional data, which are evaluated using AI algorithms to monitor equipment performance, improve production processes, predict maintenance requirements, and improve overall system reliability. These abilities allow the manufacturers to respond actively to change in production conditions while minimising the operational costs and reducing downtime [6][10]. Within food industry, AI plays an important role in improving food safety, product quality, manufacturing efficiency. AI based visual computing can automatically examine food products for faults, contamination, packaging errors, while machine learning algorithms improve the production parameters and detect abnormalities in processing functions. AI also supports smart inventory management, demand forecasting, energy optimisation, supply chain planning and allowing food manufacturers to increase the productivity while maintaining compliance with strict food safety and quality standards. The unification of AI with Digital Twin further extends these abilities by allowing constant learning, predictive analysis, and autonomous decision making. AI-Powered Digital Twins can evaluate real-time data, simulate various production scenarios, predict equipment failures and suggest best strategies before implementation in the physical environment. Therefore, AI serves as the intelligence layer of Digital Twins allowing secure, adaptive and autonomous manufacturing systems competent of meeting the evolving requirements of smart food industries [11][16].

B. Machine learning models

Machine learning (ML) composes as a key component of AI- Enabled Digital Twins allowing the smart analysis of real-time and factual manufacturing data. By understanding the patterns from the functional data, ML supports predictive maintenance, anomaly detection, quality assessment, and process optimisation. Based on their fundamental learning approach, machine learning models are used in smart manufacturing are broadly classified into three categories: Supervised learning, Unsupervised learning, Reinforcement learning [6][10].

The combination of these Machine learning models with Digital Twins paves the way for continuous learning predictive analytics, intelligent fault diagnosis and autonomous decision-making. Therefore, AI-Enabled Digital Twins can greatly enhance the operational efficiency, product quality and manufacturing resilience for intelligent food industries.

C. Predictive Maintenance:

Predictive maintenance is a high-level maintenance strategy which involves the use of real-time monitoring, Artificial Intelligence (AI), Machine Learning and Digital Twin technology to predict the failure of equipment before it happens. Unlike traditional maintenance that uses fixed maintenance schedules or repairs equipment after it breaks down, predictive maintenance relies on continuously monitoring the functional data to assess the health condition of the manufacturing equipment. This enables maintenance activities to be performed only when required, minimizing unnecessary servicing and preventing unexpected equipment failures [6][11]. AI-Enabled Digital Twins support predictive maintenance through continuous synchronisation of physical components with their virtual counterparts. Sensors embedded in manufacturing equipment collect real-time functional data including temperature, vibration, pressure, energy consumption, rotational speed and machine status. The data are sent to the Digital Twin, where AI and Machine Learning algorithms analyse the behaviour of the equipment, identify abnormal operating patterns, estimate the remaining useful life (RUL) of critical components and predict potential failures before they affect production [10][18].

In smart food manufacturing, predictive maintenance is crucial for ensuring undisturbed production and food quality. Processing equipment, including mixers, conveyor systems, refrigeration units, packaging machines, and storage facilities, must perform reliably to avoid production delays and spoilage of the product. AI-enabled Digital Twins constantly track the health of these assets and offer early maintenance recommendations, allowing manufacturers to replace worn-out parts or repair equipment before failures take place. This aggressive approach minimises production downtime, reduces maintenance costs, increases the life of the equipment and improves overall operational efficiency.

Food safety and periodic compliance are also supported via predictive maintenance by assuring that critical processing equipment is functioning within the prescribed performance limits. Manufacturers can leverage Data-Driven Maintenance decisions, optimize resource utilization and improve production reliability by utilizing AI, IoT, cloud computing and Digital Twin technology. Thus, predictive maintenance has become a basic strength of AI-enabled Digital Twins in supporting secure, intelligent and autonomous manufacturing in modern smart food industries [16][19].

D. Fault Detection

One of the complex functionalities of AI-enabled Digital Twins is fault detection, which aims to identify abnormalities, analyse equipment malfunctions and prevent failures before they affect manufacturing operations. Conventional methods of fault detection are based on periodic inspections and manual analysis, but these methods are not very good at analysis of hidden defects or detection of faults at the early stage. AI-enabled Digital Twins, however, continuously monitor equipment and production processes in real time, enabling fast detection of abnormal operating conditions and quick correction. The process of fault detection begins with the acquisition of functional data continuously from the sensors embedded in the manufacturing equipment. Industrial Internet of Things (IIoT) networks transmit parameters such as temperature, vibration, pressure, rotational speed, power consumption, and machine status to the Digital Twin.

The AI and ML algorithms are trained on these data to find the deviations from the normal operating conditions, detect the fault patterns and identify the root causes for the equipment failures. The Digital Twin can precisely determine faults and alerts ahead of critical failures by contrasting real-time data with archival records and simulation models [6][10].

Fault detection is a key function in smart food manufacturing to ensure product quality, food safety, and reduction of production losses. AI-enabled Digital Twins can detect failures in food processing equipment, refrigeration systems, conveyor belts, packaging equipment and storage facilities. Early equipment fault recognition helps to prevent contamination, product spoilage, packaging defects and unexpected production interruptions. Moreover, fault diagnosis enables maintenance teams to take corrective measures in a timely manner, thus reducing downtime and improving manufacturing reliability [11][18].

The application of AI, Machine Learning, IoT and Digital Twin technology helps to improve the accuracy and speed of fault detection significantly compared to traditional monitoring methods. AI-enabled Digital Twins provide continuous system monitoring, smart fault diagnosis and real-time alert generation, improving functional reliability, optimising maintenance planning and supporting secure autonomous manufacturing. Therefore, the capability of fault detection is vital for the development of resilient, efficient and intelligent smart food manufacturing systems [16][23].

E. Decision Intelligence

Decision Intelligence (DI) is an advanced capability of AI-enabled Digital Twins that combines Artificial Intelligence (AI), Machine Learning (ML), data analytics, and domain knowledge to support intelligent and autonomous decision-making in manufacturing systems. Unlike conventional decision-support systems that rely primarily on historical data and predefined rules, Decision Intelligence continuously analyses real-time operational data, predicts future outcomes, evaluates multiple alternatives, and recommends optimal actions to improve manufacturing performance. This enables organizations to make faster, more accurate, and data-driven decisions under dynamic production conditions.

In AI-enabled Digital Twins, Decision Intelligence uses information collected from sensors, Cyber-Physical Systems (CPS), and Industrial Internet of Things (IIoT) devices to continuously monitor manufacturing operations. Machine learning algorithms analyse the data to identify functional trends, examine system performance, evaluate vulnerabilities, simulate different production scenarios. Based on the studies, Digital Twin suggests ideal production plans, maintenance strategies, resource management plans and process adjustments. This smart decision- making ability allows the manufacturing systems to respond quickly to change the functional requirements while maintaining high-levels of productivity and efficiency [6][10].

In Smart food industries, Decision Intelligence plays a vital role in certifying product quality, food safety, adaptive capacitance. This supports manufacturers to improve the production planning, stock management, energy consumption, quality control and supply chain coordination. Additionally, Decision Intelligence assists quick responses to equipment failures, supply chain disruptions, process deviations by suggesting mitigations based on predictive analysis and real-time functional insights. These abilities facilitate to reduce food waste, production losses, and enhance overall functional reliability.

The combination of Decision Intelligence with Digital Twin technology transmutes the virtual models from Real User monitoring into analytical platforms which has the ability for autonomous operation. On integrating continuous data acquisition, Predictive analysis, optimisation and simulation, AI-Enabled Digital Twins supports enterprising and informed decision making throughout its functional lifecycle. Therefore, Decision Intelligence represents a catalyst for achieving adaptive, secure and autonomous manufacturing systems in modern Smart Food industries [18][23].

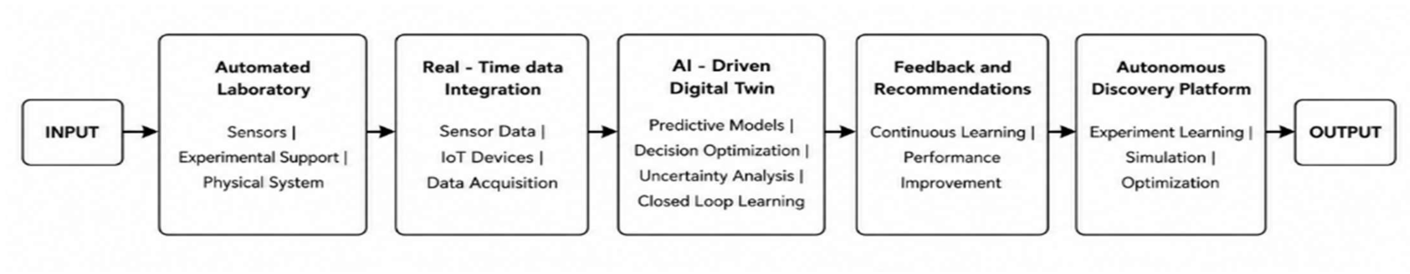

Fig 03: AI Enable Digital Twin

V. SECURITY CHALLENGES IN DIGITAL TWIN SYSTEMS

Cyber Threats to Digital Twin systems comprise of ransomware, Denial-of-Service (DoS), Malware attacks, Unauthorised access, insider tempers and data tempering. Intruders can gain access to confidential information or configure system parameters, leading to wrong decision- making, production disruptions. In the same way malware or ransomware attacks can encrypt or crook manufacturing data, interrupt production activities, and results in financial losses. Denial-of-Service (DoS) can encumber communication networks, preventing real-time data replication between physical and virtual systems and minimising the effectiveness of Digital Twin operations. In smart food industries, Cyberattacks can have disastrous outcomes beyond financial losses. Interruptions to food production, compromised traceability records, contamination risks, and unauthorized manipulation of quality data monitoring may directly affect food safety and regulatory compliance. Consequently, executing sturdy cybersecurity measures including encryption techniques, intrusion detection systems, authentication mechanisms, and constant security monitoring is important to guarantee the secure and reliable function of Digital Twin systems in autonomous food manufacturing environments [16][18].

The Industrial Internet of Things (IIoT) constitutes the communication infrastructure of Digital Twin Systems allowing constant interchange of data between physical assets and virtual components. Smart sensors, RFID devices, gateways, and connected equipment constantly gather and send functional data needed for real – time monitoring, predictive analytics automated judgement. Whereas these interconnected devices which manufacturing efficiency, and functional visibility, these also initiate several security vulnerabilities that can compromise the reliability and probity of Digital Twin Systems [10][18]. Digital Privacy is the serious problem in Digital Twin systems due to ongoing accumulation, storage, processing, and accumulating of large volumes of functional data. AI-Enabled Digital Twin depend on data generated from sensors, manufacturing equipment, Industrial Internet of Things (IIoT), and supply chain systems to construct exact virtual representations of tangible assets. This data usually consists of confidential information connected to production processes, production formulation, inventory levels, equipment performance, and business operations. Unauthorised access or Breach of such information can trade-off intellectual property, competitive advantage, and organisational security [10][18].

Data sharing among multiple partners aggravates privacy concerns. In Smart food industries, logistics providers, distributors, regulatory agencies, and suppliers mostly interchange information to guarantee supply chain transparency and product traceability. Devoid of privacy-preserving mechanisms, confidential business information may be vulnerable to unauthorised stakeholders, leading to financial loss and reduce stakeholder trust. Thus, encryption techniques, role-based access control, secure authentication mechanisms, and data governance are important for preventing confidential data from attackers while ensuring authorised data sharing. Communication Networks plays an important role in Digital Twins by real-time data synchronisation between physical assets, virtual models, IoT devices, cloud platforms.

The impact of Digital Twin rely-on integrity, accuracy, and availability of this real-time communication. Nevertheless, broadcasting massive quantities of functional data cross-device networks subjects Digital Twin systems to various communication-based attacks that can disrupt productive functions, jeopardise system reliability, and after decision attack. In smart Food Industries, communication attacks have critical consequences for product quality, food safety, and supply chain reliability. Jeopardised touchpoints may interrupt production control, traceability systems, quality assurance process, and temperature monitoring, which elevate the risk of spoilage, regulatory non-compliance, and contamination. Thus, deploying secure communication protocols, mutual authentication, continuous network monitoring, end-to-end encryption, intrusion detection systems is important to ensure secure and reliable communication within AI-Enabled Digital Twin environment. These security measures fortify the flexibility of autonomous manufacturing systems and protect analytical manufacturing functions from communication-based cyber threats [23].

The Food Industry is implementing Digital Twins, Internet of Things (IoT), Cyber Physical Systems (CPS), Artificial Intelligence (AI), to enhance food safety, supply chain management, and production efficiency. Even though, these technologies provide substantial functional perks, they also launch distinct security risks, which immediately affects product health, business continuity, and public health. Because food manufacturing comprises large number of interlinked production processes, cyber attack on one particular component can quickly affect the entire distribution and manufacturing system. Additionally, Unauthorised access, ransomware attacks, communication failures and insider threats may disrupt production operations and manufacturing efficiency. AI-Enabled Digital Twins rely on reliable and exact data for smart decision- making; that's why any compromise of data integrity or system availability can influence fault detection, predictive maintenance, and autonomous production control. In order to solve these problems, Food manufacturers should deploy cyber security measures, including end-to-end encryption, secure communication protocols, multi-factor authentication, employee security awareness, Regular security assessments, continuous network monitoring. By implementing these protective strategies, companies can reinforce the resilience of Digital Twin Systems and ensure secure, dependable, and endurable autonomous manufacturing in Smart food industries [18][16].

Threats	Description	Impact
Cyber Threats	Malware, Ransomware, unauthorised access	Interrupts the production, and data loss
Communication Attacks	MITM, Replay, DoS attacks	Communication disruption, Undependable Digital Twin synchronisation
IoT vulnerabilities	Weak security in IoT devices	Device compromise and incorrect sensor data

V. PROPOSED SECURE DIGITAL TWIN FRAMEWORK

A. *Framework Overview*

The assured Digital Twin framework is engineered to allow secure, autonomous, and intelligent manufacturing in smart Food industries. This

Framework combines Industrial Internet of Things (IIoT), Cyber Physical Systems (CPS), Edge computing, Artificial Intelligence (AI), Digital Twin Technology, and various security mechanisms into a consolidated architecture. Operational data produced by sensors are gathered and transmitted through protected communication networks to edge computing devices for preprocessing. The processed data is coordinated with Digital Twin, where AI-Based measurements perform fault detection, predictive maintenance, and process optimisation. A separate layer which is dedicated for security protects the framework by ensuring data confidentiality, secure communication, continuous monitoring, and authentication. This layered architecture enhances food safety, system reliability, resilience and operational efficiency against cyber threats while supporting autonomous manufacturing.

B. Sensor layer

The sensor layer is the bedrock for the proposed framework for constantly gathering real-time data from production machinery and environment. Sensors supervise the parameters such as vibration, humidity, pressure, temperature, machine status and energy consumption. The collected data gives an exact picture of the physical system and allow constant observation of production processes. Reliable Sensor data is important for accurate Digital Twin maintenance and also supports smart decision- making.

C. Communication Layer

The communication layer is accountable for transmitting data among edge devices, cloud platforms, sensors and the digital twin. Communication technologies like MQTT, Wi-Fi, Industrial ethernet, 5G allow reliable and real-time data interchange. Secure communication protocols ensure confidentiality, data integrity, and availability while preventing unauthorised access and reducing communication delays.

D. Edge Computing layer

The edge computing layer interprets the sensor data close to physical proximity before forwarding them to Digital Twin. Edge processing minimises communication latency, reduces bandwidth usage, and provides faster response to serious events. Edge computing also supports initial data filtering, real-time decision making, anomaly detection, thus, enhancing the reactivity of autonomous manufacturing system.

E. Digital Twin layer

The Digital Twin layer vigorously shape the virtual representation of the physical manufacturing system using real-time functional data. It constantly associated with physical assets to observe equipment performance, evaluate different operating scenarios and simulate manufacturing processes. This digital environment enables process optimisation, predictive maintenance, and strategic judgement without disrupting physical manufacturing.

F. AI- Analytics layer

The AI-Analytics layer uses Artificial Intelligence (AI) and Machine learning (ML) algorithms to evaluate functional data gathered by the Digital Twin. It assists in fault detection, predictive maintenance, demand forecasting, quality prediction and product optimisation. By decoding underlying trends and predicting future system behaviour, AI analytics allows smart and autonomous decision- making throughout the manufacturing lifespan.

G. Security Layer

The security layer safeguards the whole Digital Twin architecture against cyber threats and unauthorised access. It integrates access control, data encryption, authentication mechanisms, secure communication protocols, and intrusion detection to protect production data and system operations. This layer allows data integrity, confidentiality, and availability while maintaining the reliability of autonomous manufacturing systems.

VI. CONCLUSION

For production to be safe and independent, digital twin technology is crucial. It accomplishes this by combining several technologies, such as sophisticated data analytics, artificial intelligence, cyber-physical systems, and the Industrial Internet of Things, into a single system. The fundamentals of digital twins were covered in this section of the book. It discussed topics such as the many sorts of digital twins and how they operate. Digital twins are intended to assist the food sector monitor items in real time, anticipate when maintenance is required, identify flaws, and make informed decisions. The use of digital twins in artificial intelligence was also covered in the book. It demonstrated how machine learning models may streamline operations, raise product quality, and increase production dependability. Digital twins may be impacted by certain security concerns, such as cyberthreats and Internet of Things problems. These issues include communication system attacks and issues with data privacy. Therefore, it is crucial to implement security measures to ensure that Digital Twins can function dependably. For digital twins to continue operating, they must be secure. For the production of food, the Digital Twin framework is crucial. To keep it safe, it has numerous layers. This framework makes use of edge computing, sensors, communication networks, AI analytics, and security measures. Other concepts, such as Industry 5.0 autonomous manufacturing and blockchain integration, were also discussed. Explainable AI, sustainable manufacturing, and quantum security were also highlighted. Digital twin technology can be applied in all of these domains. As digital twin technology advances, it will be crucial for creating intelligent, robust, and sustainable production systems. Food safety will be enhanced using digital twin technology. It will improve the dependability and efficiency of manufacturing. Additionally, the Digital Twin will aid in ensuring timely delivery of supplies. In all of this, digital twin technology will be involved.

REFERENCES

1. Abdurrahman EEM and Ferrari G (2025) Digital Twin applications in the food industry: a review. Front. Sustain. Food Syst. 9:1538375. doi: 10.3389/fsufs.2025.
2. Huang, Ying, et al. "Implementation of Digital Twins in the Food Supply Chain: A Review and Conceptual Framework." *International Journal of Production Research*, vol. 62, no. 17, Sept. 2024, pp. 6400–26. *DOI.org (Crossref)*, https://doi.org/10.1080/00207543.2024.2305804.
3. Henrichs, Elia, et al. "Can a Byte Improve Our Bite? An Analysis of Digital Twins in the Food Industry." *Sensors*, vol. 22, no. 1, Dec. 2021, p. 115. *DOI.org (Crossref)*, https://doi.org/10.3390/s22010115.
4. Purlis, Emmanuel. "Digital Twin Methodology in Food Processing: Basic Concepts and Applications." *Current Nutrition Reports*, vol. 13, no. 4, Dec. 2024, pp. 914–20. *Springer Link*, https://doi.org/10.1007/s13668-024-00584-2.
5. González-Mendes, Soraya, et al. "Discovering the Conceptual Building Blocks of Blockchain Technology Applications in the Agri-Food Supply Chain: A Review and Research Agenda." *British Food Journal*, vol. 126, no. 13, Dec. 2024, pp. 182–206. *DOI.org (Crossref)*, https://doi.org/10.1108/BFJ-06-2023-0517.
6. Negri, Elisa, et al. "A Review of the Roles of Digital Twin in CPS-Based Production Systems." *Value Based and Intelligent Asset Management: Mastering the Asset Management Transformation in Industrial Plants and Infrastructures*, edited by Adolfo Crespo Márquez et al., Springer International Publishing, 2020, pp. 291–307. *Springer Link*, https://doi.org/10.1007/978-3-030-20704-5_13.
7. Tao, Fei, et al. *Digital Twin Driven Smart Manufacturing*. Academic press, 2019.

8. Moiceanu, Georgiana, and Gigel Paraschiv. "Digital Twin and Smart Manufacturing in Industries: A Bibliometric Analysis with a Focus on Industry 4.0." *Sensors*, vol. 22, no. 4, Feb. 2022, p. 1388. *DOI.org (Crossref)*, https://doi.org/10.3390/s22041388.
9. Tao, Fei, and Meng Zhang. "Digital Twin Shop-Floor: A New Shop-Floor Paradigm Towards Smart Manufacturing." *IEEE Access*, vol. 5, 2017, pp. 20418–27. *IEEE Xplore*, https://doi.org/10.1109/ACCESS.2017.2756069.
10. Tao, Fei, et al. "Digital Twins and Cyber–Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison." *Engineering*, vol. 5, no. 4, Aug. 2019, pp. 653–61. *DOI.org (Crossref)*, https://doi.org/10.1016/j.eng.2019.01.014.
11. Qi, Qinglin, et al. "Digital Twin Service towards Smart Manufacturing." *Procedia CIRP*, vol. 72, 2018, pp. 237–42. *DOI.org (Crossref)*, https://doi.org/10.1016/j.procir.2018.03.103.
12. M. Ahmadi, M. Khosravi, and H. Rahmani, "Digital Twin based Smart Manufacturing; From Design to Simulation and Optimization Schema," *Procedia Computer Science*, vol. **221**, pp. **1216–1225**, 2023. https://doi.org/10.1016/j.procs.2023.08.109
13. Fuller, Aidan, et al. "Digital Twin: Enabling Technologies, Challenges and Open Research." *IEEE Access*, vol. 8, 2020, pp. 108952–71. *IEEE Xplore*, https://doi.org/10.1109/ACCESS.2020.2998358.
14. Thelen, Adam, et al. "A Comprehensive Review of Digital Twin — Part 1: Modeling and Twinning Enabling Technologies." *Structural and Multidisciplinary Optimization*, vol. 65, no. 12, Nov. 2022, p. 354. *Springer Link*, https://doi.org/10.1007/s00158-022-03425-4.
15. Saeedi, Sarow. "Digital Twins and Their Applications in Modeling Different Levels of Manufacturing Systems: A Review." arXiv:2511.06119, arXiv, 8 Nov. 2025. *arXiv.org*, https://doi.org/10.48550/arXiv.2511.06119.
16. Henry Avila, John, and Richard De JesÃºs Gil-Herrera. "Industry 4.0 and Smart Manufacturing Convergence: Profiling Guidelines for a Fourth Revolution." *International Journal of Engineering and Technology*, vol. 9, no. 2, Apr. 2020, pp. 464–73. *DOI.org (Crossref)*, https://doi.org/10.14419/ijet.v9i2.30476.
17. Muduli, Kamalakanta, et al., editors. *Intelligent Manufacturing Management Systems: Operational Applications of Evolutionary Digital Technologies in Mechanical and Industrial Engineering*. 1st ed., Wiley, 2023. *DOI.org (Crossref)*, https://doi.org/10.1002/9781119836780.
18. Johnson, Jeffrey H. and Institute of Mathematics and Its Applications, editors. *Artificial Intelligence in Mathematics: Based on the Proceedings of a Conference on Artificial Intelligence in Mathematics*. Clarendon Press, 1994. The Institute of Mathematics and Its Applications Conference Series, N.S., 51
19. Yao, Xifan, et al. "Smart Manufacturing Based on Cyber-Physical Systems and Beyond." *Journal of Intelligent Manufacturing*, vol. 30, no. 8, Dec. 2019, pp. 2805–17. *DOI.org (Crossref)*, https://doi.org/10.1007/s10845-017-1384-5.
20. Fazlollahtabar, Hamed, and Mohammad Saidi-Mehrabad. *Cost Engineering and Pricing in Autonomous Manufacturing Systems*. First edition, Emerald Publishing Limited, 2019.
21. Yoshikawa, Hiroyuki. "Manufacturing and the 21st Century — Intelligent Manufacturing Systems and the Renaissance of the Manufacturing Industry." *Technological Forecasting and Social Change*, vol. 49, no. 2, June 1995, pp. 195–213. *DOI.org (Crossref)*, https://doi.org/10.1016/0040-1625(95)00008-X
22. "US National Academies Report Recommends Research Funding to Enhance Smart Manufacturing:

Https://Nap.Nationalacademies.Org/Catalog/27260." *MRS Bulletin*, vol. 49, no. 2, Feb. 2024, pp. 88–89. *DOI.org (Crossref)*, https://doi.org/10.1557/s43577-023-00657-7.

23. M. Nahavandi, "Industry 5.0—A Human-Centric Solution," *Sustainability*, vol. **11**, no. **16**, Art. no. **4371**, 2019, doi: **10.3390/su11164371**.
24. Chen, Baotong, et al. "Smart Factory of Industry 4.0: Key Technologies, Application Case, and Challenges." *IEEE Access*, vol. 6, 2018, pp. 6505–19. *IEEE Xplore*, https://doi.org/10.1109/ACCESS.2017.2783682.
25. Wan, Jiafu, et al. "Artificial-Intelligence-Driven Customized Manufacturing Factory: Key Technologies, Applications, and Challenges." *Proceedings of the IEEE*, vol. 109, no. 4, Apr. 2021, pp. 377–98. *IEEE Xplore*, https://doi.org/10.1109/JPROC.2020.3034808
26. Hassoun, Abdo, et al. "The Fourth Industrial Revolution in the Food Industry—Part I: Industry 4.0 Technologies." *Critical Reviews in Food Science and Nutrition*, vol. 63, no. 23, Sept. 2023, pp. 6547–63. *DOI.org (Crossref)*, https://doi.org/10.1080/10408398.2022.2034735.
27. H. Dadhaneeya, P. K. Nema, and V. K. Arora, "Internet of Things in Food Processing and Its Potential in Industry 4.0 Era: A Review," *Trends in Food Science & Technology*, vol. **139**, Art. no. **104109**, 2023, doi: **10.1016/j.tifs.2023.07.006**.
28. V. Zatsu, A. E. Shine, J. M. Tharakan, D. Peter, T. V. Ranganathan, S. S. Alotaibi, R. Mugabi, A. Bin Muhsinah, M. Waseem, and G. A. Nayik, "Revolutionizing the food industry: The transformative power of artificial intelligence—a review," *Food Chemistry: X*, vol. **24**, Art. no. **101867**, 2024, doi: **10.1016/j.fochx.2024.101867**.
29. Hassoun, Abdo, et al. "From Food Industry 4.0 to Food Industry 5.0: Identifying Technological Enablers and Potential Future Applications in the Food Sector." *Comprehensive Reviews in Food Science and Food Safety*, vol. 23, no. 6, Nov. 2024, p. e370040. *DOI.org (Crossref)*, https://doi.org/10.1111/1541-4337.70040.
30. Chhetri, Krishna Bahadur. "Applications of Artificial Intelligence and Machine Learning in Food Quality Control and Safety Assessment." *Food Engineering Reviews*, vol. 16, no. 1, Mar. 2024, pp. 1–21. *DOI.org (Crossref)*, https://doi.org/10.1007/s12393-023-09363-1.
31. Alimadani, Reza, et al. "A Review of IoT Applications in Food Processing and Related Fields." *Journal of Food Processing and Preservation*, edited by Valentina Prosapio, vol. 2025, no. 1, Jan. 2025, p. 3064441. *DOI.org (Crossref)*, https://doi.org/10.1155/jfpp/3064441
32. R. Rojo, A. L. Sanchez-Caballero, M. Sheikhalishahi, and R. S. Choras, "Integrating AI and IoT for Predictive Maintenance in Industry 4.0 Manufacturing Environments: A Practical Approach," *Information*, vol. **16**, no. **9**, Art. no. **737**, 2025, doi: **10.3390/info16090737**.
33. "AI-enabled cyber-physical-biological systems for smart energy management and sustainable food production in a plant factory," *Applied Energy*, vol. **357**, Art. no. **122334**, 2024, doi: **10.1016/j.apenergy.2023.122334**
34. H. I. Kure, S. Islam, and M. A. Razzaque, "An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System," *Applied Sciences*, vol. **8**, no. **6**, Art. no. **898**, 2018, doi: **10.3390/app8060898**.
35. Xu, Hansong, et al. "A Survey on Digital Twin for Industrial Internet of Things: Applications, Technologies and Tools." *IEEE Communications Surveys & Tutorials*, vol. 25, no. 4, 2023, pp. 2569–98. *IEEE Xplore*, https://doi.org/10.1109/COMST.2023.3297395.
36. J. Leng, S. Ye, M. Zhou, J. L. Zhao, Q. Liu, W. Guo, W. Cao, and L. Fu, "Blockchain-Secured Smart Manufacturing in Industry 4.0: A Survey," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. **51**, no. **1**, pp. **237–252**, Jan. 2021, doi: **10.1109/TSMC.2020.3040789**.

37. B. İnanlar and F. Altay, “Digital Twin Technology in AI-Operated Metaverse for Food Processing: A Pathway to Sustainability, Efficiency and Innovation,” Trends in Food Science & Technology, vol. 168, Art. no. 105491, 2026, doi: 10.1016/j.tifs.2025.105491.
38. Q. Qi and F. Tao, “A Smart Manufacturing Service System Based on Edge Computing, Fog Computing, and Cloud Computing,” IEEE Access, vol. 7, pp. 86769–86777, 2019, doi: 10.1109/ACCESS.2019.2923610
39. Ren, Lei, et al. “Cloud Manufacturing: Key Characteristics and Applications.” International Journal of Computer Integrated Manufacturing, vol. 30, no. 6, June 2017, pp. 501–15. DOI.org (Crossref), https://doi.org/10.1080/0951192X.2014.902105.
40. Lin, Chun-Cheng, et al. “Smart Manufacturing Scheduling With Edge Computing Using Multiclass Deep Q Network.” IEEE Transactions on Industrial Informatics, vol. 15, no. 7, July 2019, pp. 4276–84. IEEE Xplore, https://doi.org/10.1109/TII.2019.2908210.

