Preprints.org

Review

Not peer-reviewed version

# Digital Twins, AI, and Cybersecurity in Additive Manufacturing: A Comprehensive Review of Current Trends and Challenges

Md Sazol Ahmmed , Laraib Khan , Muhammad Arif Mahmood , Frank Liou *

Posted Date: 30 June 2025

doi: 10.20944/preprints202506.2516.v1

Keywords: digital twin; artificial intelligence; cybersecurity; blockchain; additive manufacturing

 doi:10.20944/preprints202506.2516.v1



*Review*

# Digital Twins, AI, and Cybersecurity in Additive Manufacturing: A Comprehensive Review of Current Trends and Challenges

**Md Sazol Ahmmed [1], Laraib Khan [1], Muhammad Arif Mahmood [2] and Frank Liou [1,*]**

[1] Department of Mechanical and Aerospace Engineering, Missouri University of Science and Technology, Rolla, MO 65409, USA
[2] Intelligent Systems Center, Missouri University of Science and Technology, Rolla, MO 65409, USA
* Correspondence: liou@mst.edu

**Abstract**

The development of Industry 4.0 has accelerated the adoption of sophisticated technologies, including Digital Twins (DTs), Artificial Intelligence (AI), and cybersecurity, within Additive Manufacturing (AM). By enabling real-time monitoring, process optimization, predictive maintenance, and secure data management, which are redefining conventional manufacturing paradigms. Although their increasing individual importance, a consistent understanding of how these technologies interact and collectively improve AM procedures is lacking. Focusing on the integration of digital twins (DTs), modular AI, and cybersecurity in AM, this review presents a comprehensive analysis of over 102 research publications sourced from Scopus, Web of Science, Google Scholar, and ResearchGate. The publications are categorized into three thematic groups, followed by an analysis of key findings. Finally, the study identifies research gaps and proposes detailed recommendations along with a framework for future research. The study reveals that traditional AM processes have undergone significant transformations driven by digital threads, digital threads (DTs), and AI. However, this digitalization introduces vulnerabilities, leaving AM systems prone to cyber-physical attacks. Emerging advancements in AI, Machine Learning (ML), and Blockchain present promising solutions to mitigate these challenges. This paper is among the first to comprehensively summarize and evaluate the advancements in AM, emphasizing the integration of DTs, Modular AI, and cybersecurity strategies.

**Keywords:** digital twin; artificial intelligence; cybersecurity; blockchain; additive manufacturing

---

## 1. Introduction

The adoption of innovative technologies associated with Industry 4.0, often referred to as the fourth industrial revolution, is driving a significant shift in the manufacturing industry. One of the most significant developments from the more traditional rapid prototyping technique is metal additive manufacturing (MAM) [1,2]. For instance, the GE9X engine used in the Boeing 777X has reduced the number of components that make up a heat exchanger assembly from 300 to just one, resulting a cheaper and more lightweight solution [3]. As this technology has developed over time, it has become abundantly evident that the phrase "rapid prototyping" does not adequately describe its capabilities. As opposed to traditional methods, MAM creates components, in a layer-by-layer fashion, using materials such as metal wire or powder based on 3D designs. This process requires minimum interaction from humans [4]. The American Society for Testing and Materials (ASTM) and the International Standards Organization (ISO) claim that seven primary forms of MAM techniques exist. From aerospace to medicine to tools and consumer products, powder bed fusion (PBF) finds applications in many diverse sectors. To create the intended shape, powder particles are heated or sintered under an energy source [5]. PBF technology may be further classified in part by the powder melting techniques they use: While electron beam melting (EBM) defines machines that employ electron beams, the two primary types of laser-based machines are selective laser melting (SLM) and selective laser sintering (SLS) [6]. Directed energy deposition (DED) is a typical technique for either adding or repairing material to already-existing components [7]. Similar to PBF, this method utilizes lasers for fusion and can operate on either wire or powder. DED differs only in that the printhead typically serves as both the feedstock and the energy source. The system names for DED machines running powder are laser metal deposition (LMD), wire arc additive manufacturing (WAAM), and electron beam additive manufacturing (EBAM), respectively [8].

In the scene of AM in this age of Industry 4.0, a significant shift to more modern technologies is underway. Cybersecurity [9], modular AI [10], and the digital twin (DT) [11,12] have evolved into essential elements that help improve the reliability and efficiency of industrial operations. DT technology enables manufacturers to create real-time virtual replicas of their physical assets, thereby facilitating proactive optimization and continuous performance monitoring. Conversely, modular AI offers flexible modules tailored to specific tasks, enhancing processes and refining decision-making abilities 10, 11]. As the number of networked systems continues to increase, it is more crucial than ever to implement stringent cybersecurity measures to safeguard irreplaceable intellectual property and ensure the integrity of industrial processes against cyberattacks [9,13,14]. These advances not only optimize resources but also enhance operational effectiveness, allowing organizations to create unique products unlike those of past years. Still, the adoption of these concepts raises serious challenges [15–17].

Especially in industries such as aerospace, metal AM is beginning to challenge established wisdom and may change traditional manufacturing by looking at the GE9X engine [3]. This meets the high-performance criteria specified by the aviation sector, while also reducing manufacturing costs and assembly times. Still, producers must apply rigorous quality assurance procedures to make sure that every item fulfills or surpasses criteria because materials vary. In addition, DT technology provides even another useful tool for the toolbox by allowing producers to create virtual versions of their assets in real-time [18]. They might therefore demonstrate initiative in implementing changes and monitoring the situation of things. IoT devices and sensors enable firms to quickly enhance their operations and identify inefficiencies as they collect vital data from their industrial activities [19]. Notwithstanding their difficulties, mass data management projects and computing capacity are required to accurately represent these systems and integrate them with the existing IT infrastructure. Additionally, modular AI offers algorithms tailored to specific industrial needs, thereby enhancing product performance. These AI modules might explore vast amounts of data in search of trends to aid in streamlining processes [20]. By predicting when equipment is likely to break, ML enables quick repairs, thereby helping to better control manufacturing. Still, using AI presents problems [21,22] related to data privacy, the need for high-quality training data, and the possibility of algorithmic bias that could complicate judgments. As manufacturing becomes increasingly networked, strong cybersecurity is crucial to protect private information and ensure that operations proceed as expected [23]. Businesses dependent on advanced security systems run the danger of being targets for hackers able to compromise data and disrupt operations. Organizations must continually adapt their security strategies to match the evolving nature of cyber threats, which can be financially taxing [23,24].

Although much has been accomplished in the fields of DTs, AI, and cybersecurity separately, their combined influence in changing AM, especially MAM, remains underexplored in current research. These technologies used together could unleash hitherto unrealized degrees of predictive maintenance, real-time process optimization, and system security. Most current research, however, examines these technologies separately without a consistent framework addressing their synergy, interdependencies, and implementation difficulties in industrial AM systems. Furthermore, as AM becomes more data-driven and networked under Industry 4.0, new risks and operational complexities surface, necessitating comprehensive plans. This emphasizes the urgent need to

 doi:10.20944/preprints202506.2516.v1



synthesize the current research situation, identify technical gaps, and propose integrated solutions. Future research needs to be guided by industry best practices and supported by the creation of robust, intelligent, and safe AM systems through a targeted, multidisciplinary assessment.

This work attempts to give a comprehensive analysis of the ways in which DT, modular AI, and effective cybersecurity technologies might greatly improve AM processes in the transforming terrain of Industry 4.0. Focusing on these new technologies will allow us to investigate their synergies and cumulative impact inside industrial environments. By focusing on these new technologies, we will examine their synergies and cumulative effects within the context of industrial settings. This will help to better grasp their influences on operational efficiency, product customization, and decision-making.

Furthermore, this research will examine the challenges that prevent the effective implementation of these developments and provide an understanding of how professionals in the area can overcome them. The review paper is organized into several interconnected sections, reflecting the concepts expressed in the introduction, to simplify the process of conducting this research. DT technology will be thoroughly discussed in Section 2, with its applications in manufacturing process improvement, primarily in-time performance monitoring and proactive optimization, highlighting its benefits. This part will be based on the already mentioned introduction. Modular AI will be discussed in Section 3, along with its applications in data analytics, predictive maintenance, and the enhancement of operational decision-making capabilities. Section 4 will emphasize the importance of cybersecurity techniques in safeguarding industrial processes against the growing number of cyber hazards resulting from the increasing interconnection of industries. Section 5 will address the challenges that prevent the application of these technologies and offer remedies to overcome them. Section 6, a summary of the most significant results, will be presented in the final part of the study, along with an outline of future research directions aimed at enhancing the robustness and efficiency of AM through the use of DTs, modular AI, and cybersecurity solutions.

## 2. Digital Twin Technology in Additive Manufacturing

Digital Twin (DT) technology is emerging as a key pillar for achieving several benefits in the era of Industry 4.0, as sectors such as manufacturing undergo digital transformation [1]. Although DT technology originated in the aerospace sector [25], where it was used to replicate and track space spacecraft, its ability to transform other sectors is becoming increasingly clear. DT provides applications spanning design, optimization, maintenance, decision-making, and training; it also enables the linking of physical and virtual worlds in real time, thereby providing a more realistic and comprehensive perspective of operations [3]. DT is a great tool for improving productivity, competitiveness, and efficiency as it allows one to replicate, track, and forecast system performance. Within AM, DT technology holds great promise, as it enables the use of virtual duplicates of machinery and processes. By doing so, companies can increase productivity, minimize time to market, reduce maintenance-related costs, and enhance product quality [26]. As businesses have come to depend more on digital solutions for remote monitoring and maintenance, the COVID-19 pandemic has accelerated the adoption DT in the industry [4]. Although the idea of DT is not entirely novel, it originated in early concepts of Product Lifecycle Management (PLM) and NASA's innovative applications [5]. Its integration with advanced computing, IoT, and AI in modern manufacturing processes has unlocked a new level of operational efficiency [6,8]. DT helps precisely monitor complex production processes by creating virtual replicas of actual physical facilities in the AM, thereby enabling condition-based predictive maintenance, proactive decision-making, and better product customization. As AM advances, the impact of DT on it is expected to grow, thereby promoting creativity and altering accepted industrial patterns.

Zhang et al. presented a logical overview of DTs in AM, which is illustrated in Figure 1. This model consists of mechanical models, control models, and some statistical models besides ML models and big data. This framework acts as a base of DT application in AM [9]. Various researchers used

 doi:10.20944/preprints202506.2516.v1



different DT frameworks in their research, and Table 1 illustrates different DT application AM and shows the author's contributions with the future scope.

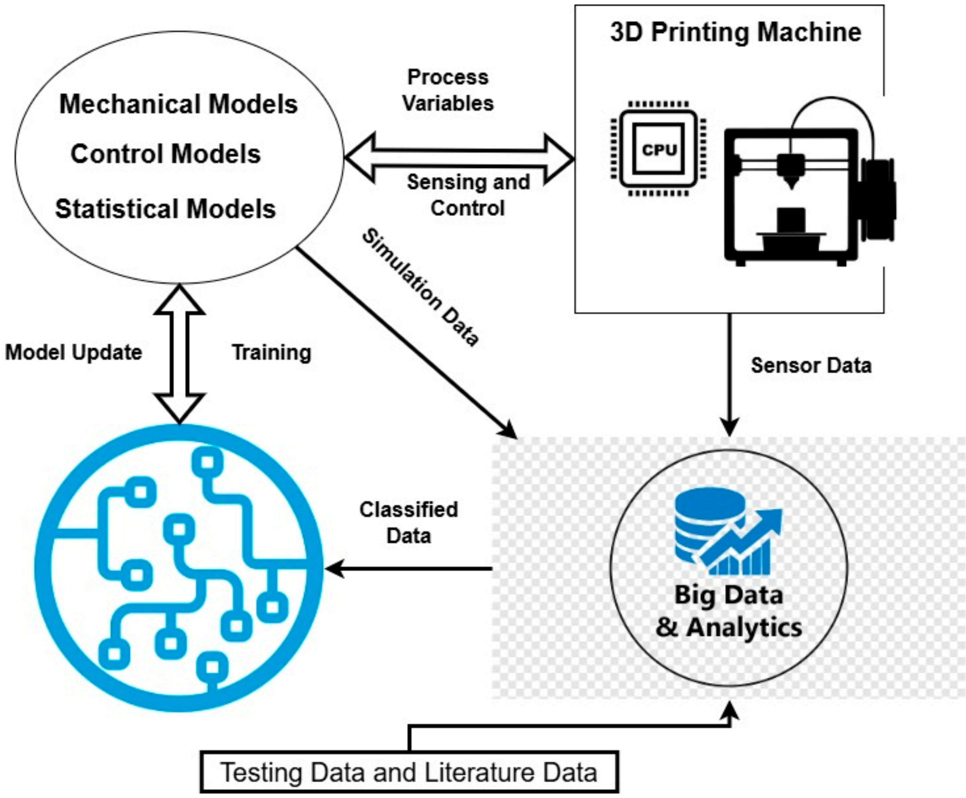



**Figure 1.** General framework of DT applications in AM; based on the data [9].

**Table 1.** DT current state in different AM applications.

| Reference | Contributions | Future scope |
|---|---|---|
| [10] | • DT framework for AM<br>• Generalizable methodology of DT applications for AM processes like LBPF and DED<br>• Enhanced defect detection with gray-box modeling through DT application | A single in-situ sensor monitors only temperature distribution but additional process parameters such as laser power, scan speed, layer thickness etc., can extend the accuracy of flaw detection across various AM methods |
| [12] | • It was shown how dynamic data-driven application systems enabled the implementation of a feature re-ranking method able to help sustain the current state of the DT | Advanced AI and ML Integration with cyber-physical systems can improve real-time data analytics capabilities to facilitate predictive insights |
| [11] | • It is shown that cooperative data management made possible by DT has great potential to advance basic knowledge of metal additive manufacturing techniques<br>• Developed simulation and prediction models can reduce development times and costs and improve production efficiency | The DT-enabled collaborative data management system can have ML-enabled advanced data analytics developed and implemented and applied in it |
| [13] | • Presented a novel framework for predicting melt pool behavior | Implementing predictive models that can adapt in real time to changing conditions during the AM process is a significant |

| | | |
|---|---|---|
| | • Robust predictive model for spatial and temporal variations in metallurgical parameters | challenge. It needs more validation and a verification process |
| [14] | • It identifies the essential building blocks necessary for constructing a robust DT | The development of a comprehensive database and Quantitative study of solidification texture can be explored |
| [18] | • It is shown that a 3D printing machine with mechanical, control, and statistical models designed holistically can lower defect count and cut the time interval between the design and production stages | Enhanced data integration and open-source collaboration can improve the DT applications in AM |
| [19] | • It provides a framework for the implementation of augmented reality and DT in AM | To improve the AM process chain, it is crucial to guarantee the validity and verifiability of the possible basic self-learning strategies as well as to better control data |

Furthermore, Phanden et al. demonstrated that integrating a DT into AM requires four fundamental elements, as illustrated in Figure 2: AI, big data analytics, machine configuration based on the DT, and the DT models themselves. First, the AM equipment is painstakingly set up to account for temperature and laser power, among other factors. Furthermore, the attached sensors are used to gather real-time data. The DT models, which replicate physical processes, track geometric aspects, and assess past data to identify patterns, are fed into this data. Big data analytics helps identify anomalies in real time, thereby allowing for speedy repairs. AI algorithms help to enhance this process by allowing one to predict future issues and automatically modify operating parameters if deviations occur. This integrated approach not only improves the quality and consistency of the produced components but also ensures that the process is more efficient, thereby reducing the number of mistakes that arise and guaranteeing that the products adhere to the design criteria [20]. Chen et al. developed multi-sensor-based DT in AM for in-situ quality monitoring. In this case, they used multisensory fusion to get a more complete understanding of the fundamental process of physics, such as porosity and the growth of it. Some examples of the sensor-captured process data included in robotic DED are coaxial melt pool images, temperature fields, audio signals, and a three-dimensional point cloud on the component surface. Typically, spatial-temporal data fusion is employed to synchronize and register multisensory features, which are the primary contributions in this discipline.

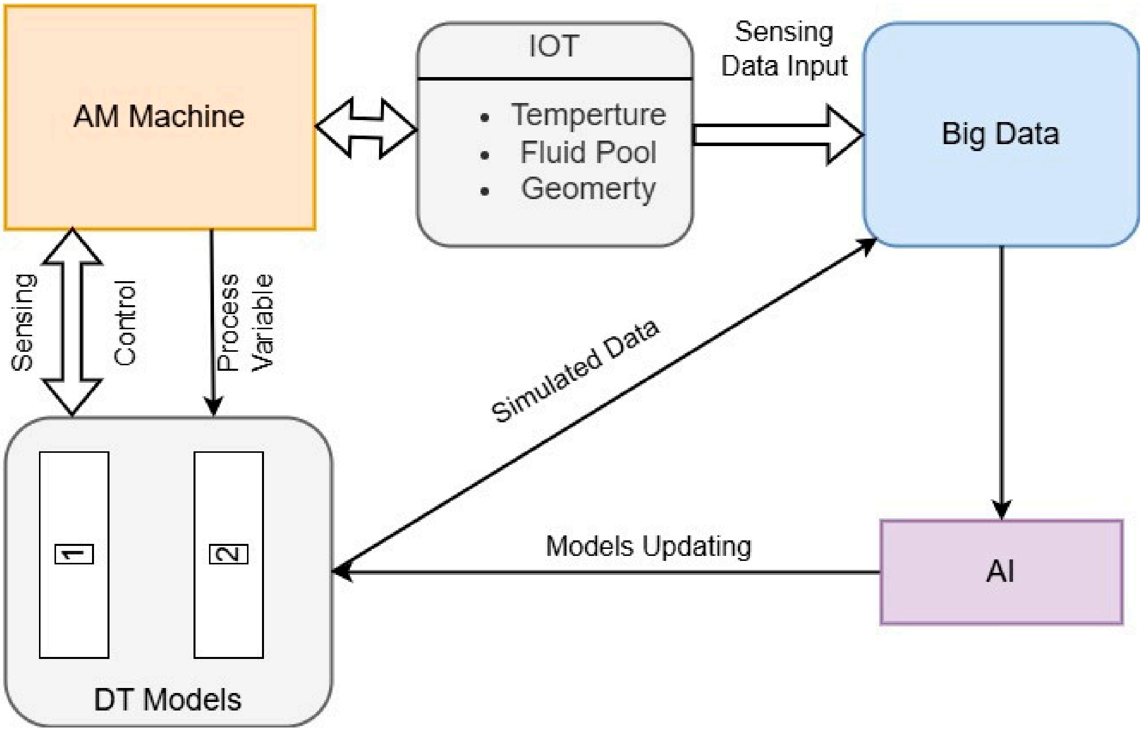



**Figure 2.** Representation of DT Implementation in AM; based on the data [20].

Figure 3 illustrates the entire setup procedure for using multiple sensors. After the LDED process, data from multiple sensors are fused in time and space and resampled at 250 Hz to match the robot's position data, allowing for detailed quality mapping. Microscopy reveals distinct defects at different part layers, such as keyhole pores in upper layers and cracks in the middle, with these defect types associated with specific sensor features like melt pool width. Each sensor exhibits varying effectiveness in detecting defects, as evidenced by the omission of certain cracking signals identified by melt pool features. This fused data will support training ML models to predict defect locations within the part [27].

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2025 doi:10.20944/preprints202506.2516.v1



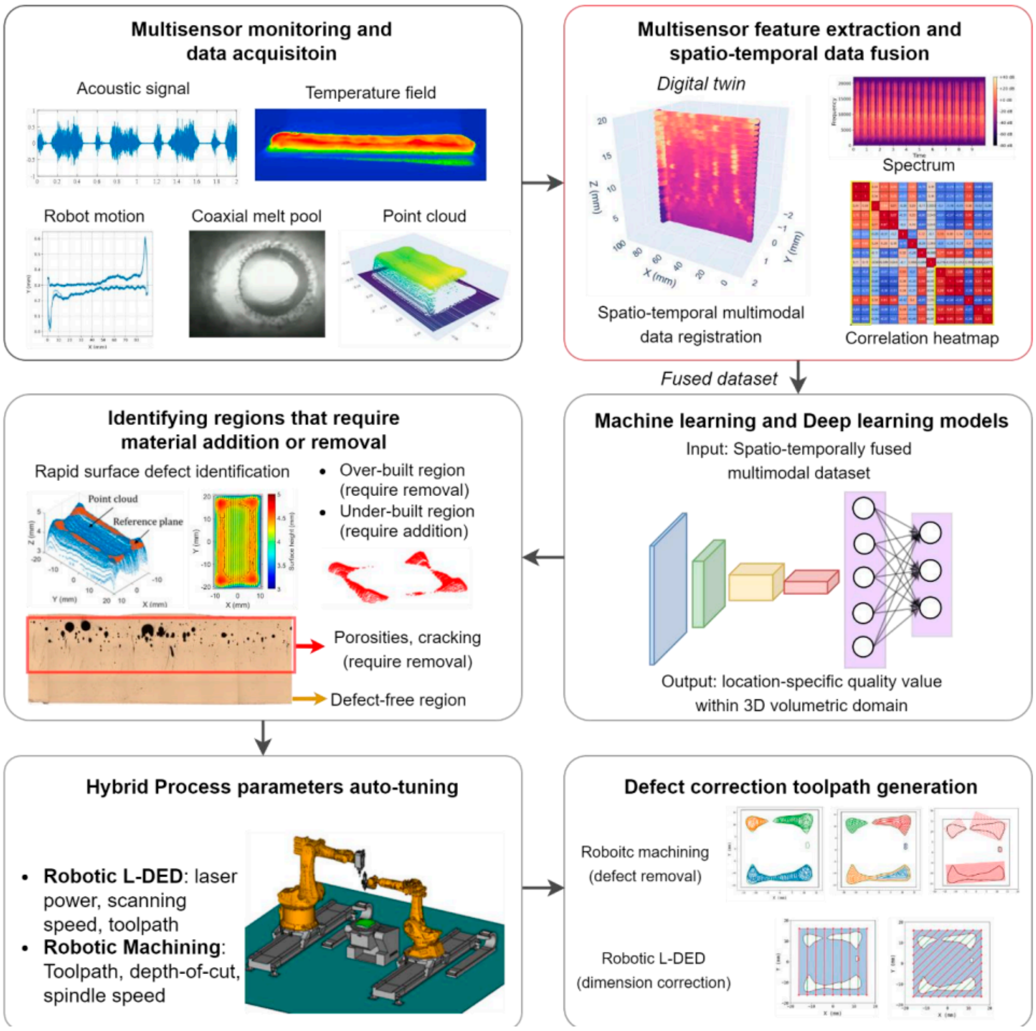



**Figure 3.** Multisensory DT in robotic LDED AM for in-situ quality monitoring based on the data (Chen, Yao, et al., 2023).

Based on a five-dimensional DT model, Xu et al. proposed an Augmented Reality-assisted Cloud AM (AR-CAM) architecture that integrates actual goods, virtual replicas, data, services, and networking, as illustrated in Figure 4. Through centralizing and distributing real-time data on a Cloud Manufacturing platform, the system improves data security and resource allocation. Utilizing improved and customized products throughout several phases, this setup helps visualize various manufacturing techniques in AR. AR-CAM also promotes a shared knowledge base by facilitating prototyping and knowledge-sharing to speed product upgrades and improve demand responsiveness [22]. For toolpath planning and simulation, Yi Cai et al. also presented an AR-based method to efficiently transfer layout information between a reconfigurable AM system with robotic arms and its DT. Using transformation matrices to establish interactions between the camera, markers, robotic arms, and substrate [23], a prototype system with two desktop robotic arms proved the potential of the approach to automatically recover spatial data.

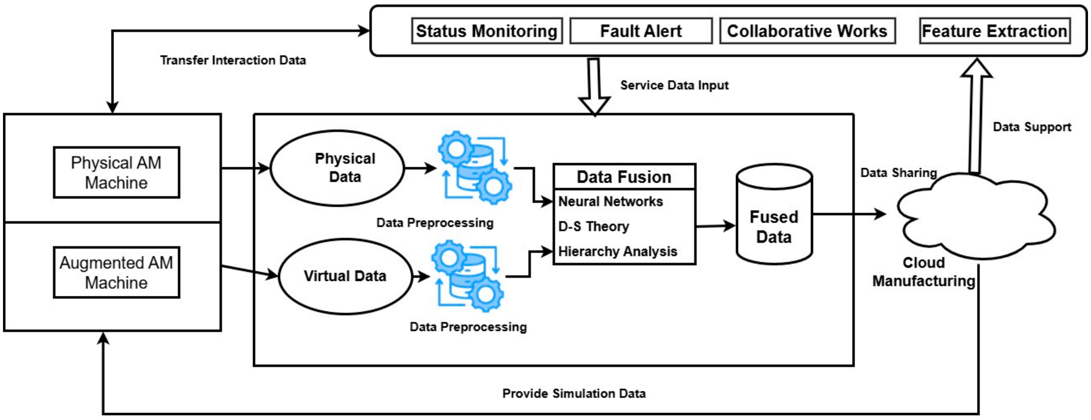



**Figure 4.** The framework of augmented reality-assisted cloud AM; based on the data [22].

Phua et al. also contributed by proposing a hierarchical framework for developing DTs specifically for metal AM, categorizing them into four levels of increasing complexity. This hierarchy consists of surrogate modeling, in-situ sensing, hardware control, and intelligent control policies needed to achieve effective, real-time control of the AM process. Another issue the authors addressed was the "intelligent DT" level displayed in Figure 5, where better control rules allow independent, adaptive decision-making, free from influence. Seeking to maximize print quality, defect management, and design customizing, this offers a uniform platform for aggregating simulations, sensor data, and control systems. Promoting more universal scalability and integration in industrial settings, the framework also provides concepts pertinent to several AM approaches and advanced manufacturing systems [24].

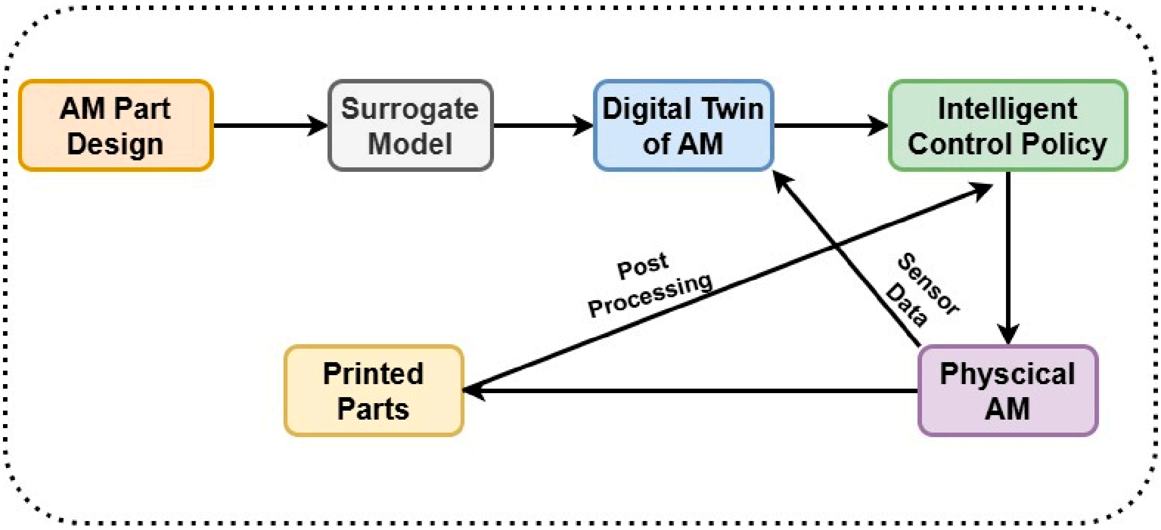



**Figure 5.** Framework for the Intelligent DT; based on the data [23].

Based on the various literature summaries of DT development in AM, it has become clear that DT integration with AI has played a significant role in data management, early fault detection, in-situ monitoring, and sensor data analysis. So, the next section will briefly discuss the role of AI in AM system reconfiguration and optimization.

## 3. Modular AI for System Reconfiguration and Optimization (AI/ML Algorithms)

AI has revolutionized AM by enhancing and ensuring the quality of production processes and products [28]. With flexible and adaptable technology and modular AI, manufacturing companies can respond quickly to evolving manufacturing needs and challenges. Within the scope of in-situ process monitoring, material and process optimization, workflow automation, and real-time decision-making, AI is a highly valuable technology [28–30]. AI models, for example, can dynamically adjust machine parameters while the machine is running [31], assess sensor data tidentify flaws or anomalies, optimize resource usage to minimize waste, and autonomously perform industrial processes. This adaptability also drives predictive maintenance by enabling the analysis of machine data to identify problems, thereby saving downtime and extendingquipment lifetime [32,33].

Data collection, AI model building, dynamic algorithms, and feedback systems collectively ensure efficient manufacturing throughodular AI-driven optimization frameworks [34]. Real-time preprocessing of sensor data for training ML models maximizes process parameters including laser power, layer thickness, and printing speed [35,36]. These models change over time using feedback loops, which also contribute to making production even more dependable. Modular AI systems increase versatility by easily changing for different materials, setups, or production goals. Tools including DTs, cloud computing, and edge computing further help AI-driven optimization by providing simulations, large-scale data processing, and low-latency decision-making.

AI-powered automation has streamlined AM processes, increased productivity, and enabled innovative ideas to flourish. For example, AI-driven vision systems can detect manufacturing defects, thereby saving inspection time and improving standards. Dynamic process reconfiguration enables systems to adjust parameters in real time, depending on ambient conditions or material properties. Likewise, mass customization driven by AI enables the scalable production of tailored components without compromising manufacturing efficiency. Table 2 depicts the different AI models used in AM development.

**Table 2.** AI Model Contribution in Development of AM.

| Reference | AI Model | Contribution in AM (What they did and what are the results) |
|---|---|---|
| [37] | ANN | AI into AM, leading to the development of closed-loop AM systems and DTs |
| [38] | Deep learning | A smart AM framework based on cloud-edge computing |
| [39] | ML | an innovative approach for online quality monitoring of AM employing acoustic emissions |
| [40] | AI | The osmotic manufacturing method was proposed as a concept to apply additive manufacturing techniques together with graph theory |
| [41] | Deep learning | A real-time computing-based self-monitoring system has been designed to classify the several degrees of delamination that could arise in a printed part |
| [42] | ML and Deep learning | An overview of AI in AM for a closed-loop system is presented |
| [43] | AI | Shows how artificial intelligence may increase design efficiency, help discover materials, maximize additive manufacturing techniques, and guarantee the quality of outputs generated by AM |
| [44] | A generalizable AI | A fully automated workflow across several AM systems should be used for the aim of supporting quick autonomous process parameter discovery and/or enhanced scientific understanding |
| [45] | AI | It speeds up simulations, improves the selection of materials, facilitates the design of novel structures with multiple functionalities, and cuts down on both time and money spending |

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2025 doi:10.20944/preprints202506.2516.v1



While discussing with DTs and AI in AM, it means that it opens the opportunity to utilize cyberspace for better PLM in AM. However, the management of cyberspace is important as it integrates lots of digital threads, sensors, and networks. The next chapter will discuss cyber security considering different cyber attacks in AM and possible solutions.

## 4. Cyber Security in Additive Manufacturing

A Cyber Manufacturing System envisions fully integrated physical and computational processes in a connected manufacturing ecosystem. By leveraging IoT [24,46], cloud computing [47], ML [48–51], sensor networks [50,51], and advanced manufacturing, these systems enable smart capabilities like self-awareness, self-prediction, and self-organization, fostering a responsive and adaptive production environment [52,53]. In this context, AM significantly expands design flexibility, supporting complex geometries that conventional methods cannot achieve [54]. Cyber-enabled AM platforms further enhance capabilities through rapid communication, iterative design updates, and remote information sharing on setup and processing parameters [55,56]. However, this interconnectedness also heightens the risk of cyber-physical attacks, presenting critical security challenges in the deployment of cyber-physical AM systems [57,58]. This section covers the research articles on cyber-physical attacks in manufacturing, covering incident investigations, and research studies. Intrusion detection approaches are examined across the cyber-physical manufacturing domains. Additionally, physical detection methods that use side-channel data—such as acoustic signals, imagery, and acceleration—to detect attacks during manufacturing processes are discussed.

Figure 6 illustrates a taxonomy of attacks in Cyber manufacturing systems based on the data [59,60]. The influenced area represents where attacks originate or target first. In the cyber domain, attacks can compromise servers, files such as STL and G-code (used in 3D printing), cloud-based manufacturing systems, and wireless sensor networks. In the physical domain, attacks could affect raw materials, parts, assemblies, equipment, and machines, as well as the power supply needed for operations. Victim elements represent areas impacted by the attacks, either directly or indirectly due to compromised influenced elements. In the cyber domain, attacks compromise sensor data, ML processes, intellectual property, and real-time simulation capabilities. In the physical domain, the impacts extend to final products, human safety, the functioning of equipment and machinery, and customer satisfaction and loyalty. Table 3 illustrates major attacks classification, sub classification, existing remedy

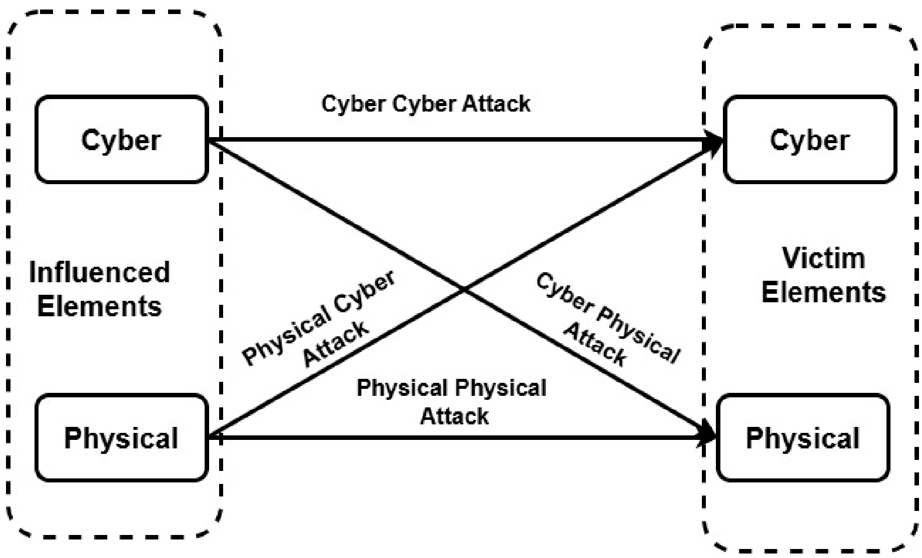



**Figure 6.** Taxonomy of attacks in cyber manufacturing systems based on the data [59–61].

**Table 3.** Major Attacks Classification and Existing Solutions.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2025 doi:10.20944/preprints202506.2516.v1



| Major Attacks | Subcategory Attack | Attack Model | Existing Solutions | Reference |
|---|---|---|---|---|
| Hardware Attacks | Side channel attacks | Acoustic Analysis, Electromagnetic Attacks, Power Analysis, Data Residuals, Environmental Exploits, Trimming Exploits, Cache Side-Channel, Differential Faults | • Antivirus<br>• Software update<br>• Multi-factor authorization for access control<br>• Firewall/gateway/proxy Data encryption<br>• Data streams encryption<br>• Encryption of communication<br>• Secure communication (e.g., VPN, Wi-Fi, etc.) | [62–68] |
| | Physical attacks | Physical Damage, Chip Decapsulation, Node Jamming, Node Tampering, Fake Node Injection, Code Injection, Sleep Deprivation Attack RF Interference | | |
| | Network attacks | Outage attacks, DoS, tag cloning, camouflage, Man in the Middle, micro probing, traffic analysis, object replication | | |
| | Data Attacks | Data exposure, leakage, loss, and scavenging; account hijacking; brute force; hash collision; malicious VM (virtual machine); and VM hopping | | |
| Software Attacks | Firmware attacks | Malware, reverse engineering, control hijacking, eavesdropping | | |
| | Operating system attacks | Malware, worm, virus, Trojan, phishing, brute force, back door | | |
| | Web application attacks | Malware, spyware, DDoS, pathbased DoS, reprogram attacks, malicious code injection, exploitation for reconfiguration | | |

Table 4 summarizes the various types of cyber-attacks in AM and the possible solutions authors experimented with in their studies.

**Table 4.** Cyber-physical Attack in AM.

| Reference | Attack Type | Detection Method | Result |
|---|---|---|---|
| [69] | Malicious void Consequence | The effect on the mechanical strength of a printed specimen was investigated by means of a "printed void" | 14% reduction in yield load |
| [70] | Dimensions Change | Developed the Bayesian game, computing Bayes-Nash equilibria | Operators under attack were not aware of |

| | | | |
|---|---|---|---|
| | | | dimensional change without reminding |
| [71] | Printing orientation | Mechanical testing, finite element analysis, and ultrasonic inspection | Strength, failure strain reduction |
| [55] | Malicious void Consequence | Presented DTs utilizing data-driven ML models, and physics-based models | Drone propeller fatigue life reduction |
| [72] | Inside the hole of a solid block | • LSTM-autoencoder for data extraction<br>• Many ML Models both supervised and unsupervised | • LSTM-AE+ AdaBoost shows higher accuracy for supervised learning<br>• LSTM-AE +OCSVM-EWMA for unsupervised monitoring |
| [59] | Different infill defect patterns | RNN, Random Forest, and anomaly detection | The accuracy of anomaly detection is 96.6% |
| [73] | Alternation of G code | Audio fingerprint comparison | The detection rate of the deviation at the time of its occurrence was 100% |
| [74] | Vulnerability in critical components named Gear and Wrench | ML Model | Proposed robust detection systems to prevent structural failures |

Wu et al. [59] demonstrated a vision-based security mechanism in a 3D printing setup to detect and alert administrators of potential defects in real time. Five different infill defect patterns were designed: seam, irregular polygon, circle, rectangle, and triangle to simulate attacks. The proposed framework using supervised ML helps to detect the attack more accurately and speedily. The entire process, from image capture, syncing, downloading, feature extraction, classification, and alert generation, took around 1 minute, although network conditions may affect this timing. Anomaly detection has been found more accurate method among RNN, Random Forest, and anomaly detection. The accuracy of anomaly detection is 96.6%.

Shi et al. [72] discussed the limitations of current monitoring methods, which focus on process anomalies such as material flow or overheating but often miss cyber-physical attack-induced alterations. Different key challenges have been found including difficulty measuring certain process attributes, the complexity of AM physics, and the vast, unpredictable range of possible process alterations. This work presents a feature extraction method based on LSTM-autoencoder to efficiently capture the attack-induced changes in online collected sensor signals; its suggested framework is shown in Figure 7.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2025 doi:10.20944/preprints202506.2516.v1



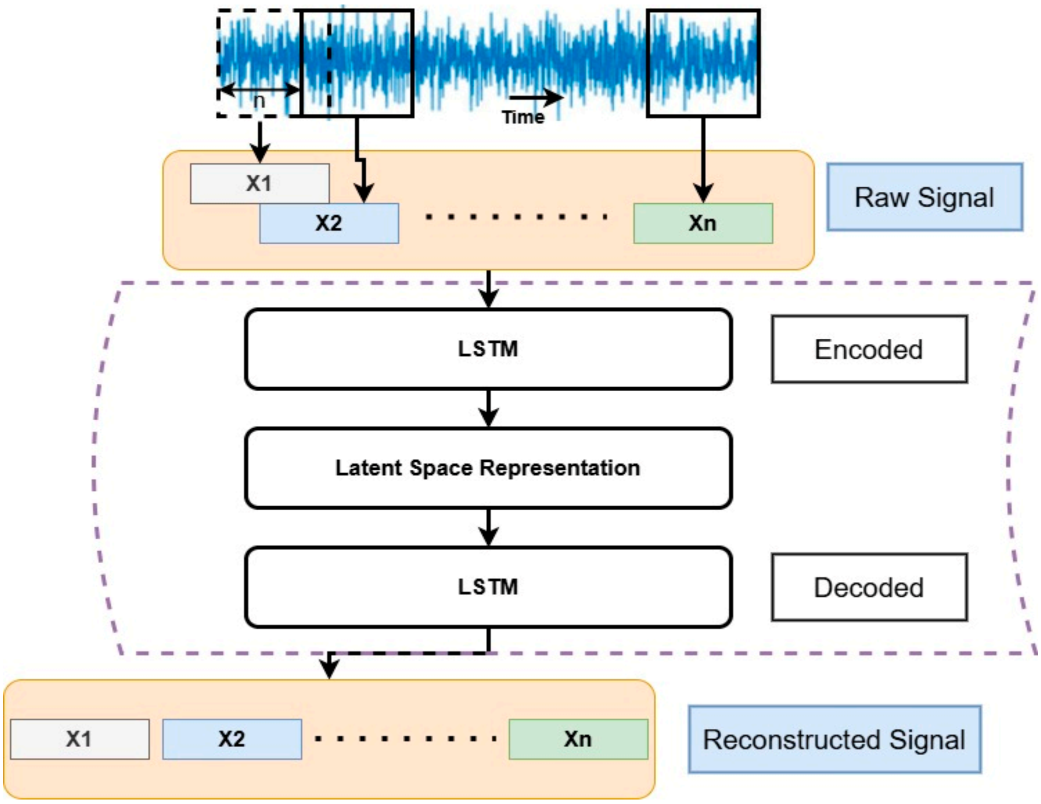



**Figure 7.** Proposed Framework for Feature Extraction Approach; based on the data [72].

Two potential cyber-physical attack scenarios were investigated to validate the monitoring approach, with design parameters:

Case 1: Attack on the design geometry in the "STL" stage aimed at adding a little square-shaped void in the construction. In 1 to 41 layers kept solid but 42-67 layers had a square hole inside.

Case 2: During the "slicing" stage, the layer thickness was taken into consideration to modify the thickness of particular layers. In case 02, layers 1-40, 41-56, and 57-67 thickness were 0.3 mm, 0.25 mm and 0.35 mm respectively.

After capturing data and data extraction, they implemented both unsupervised and supervised monitoring approaches for online cyber-physical attack detection. Among different algorithms, for both case 01 and, LSTM-AE+ AdaBoost showed a higher score in precision, Recall, and F-score that is 0.9479, 0.9460, and 0.9469, respectively for case 01 and 0.9477, 0.9790, 0.9631 respectively. Moreover, they also proposed LSTM-AE +OCSVM-EWMA for unsupervised monitoring. Sofia Belikovetsky et. al [73] concentrated exclusively on sabotage attacks, proposing a detection method using side-channel audio verification to enhance AM security against cyber-physical threats as shown in Figure 8. They proposed a Detection Method that's workflow:

- STL or G-code file of the object produced in a lab environment.
- The audio signal was recorded during manufacturing.
- The audio fingerprint was calculated, encrypted, and appended to the G-code file.

Then, they compared the sound generated during the new manufacturing process to the signed audio fingerprint to verify the object's authenticity.

doi:10.20944/preprints202506.2516.v1



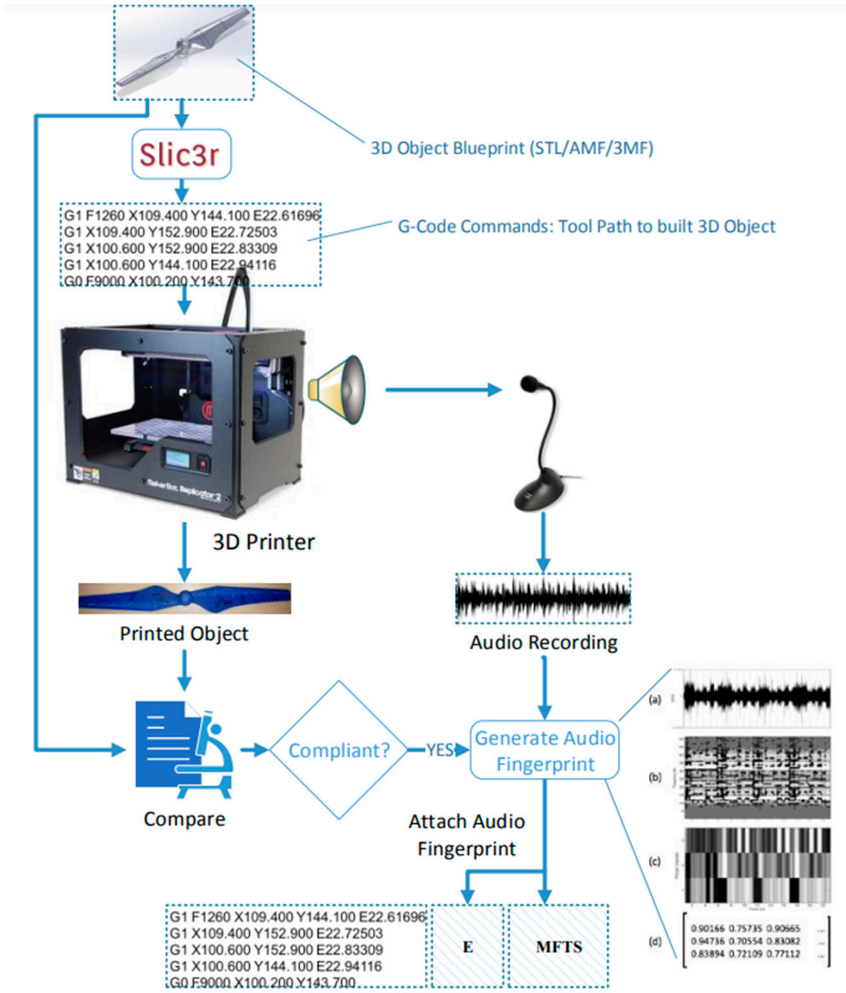
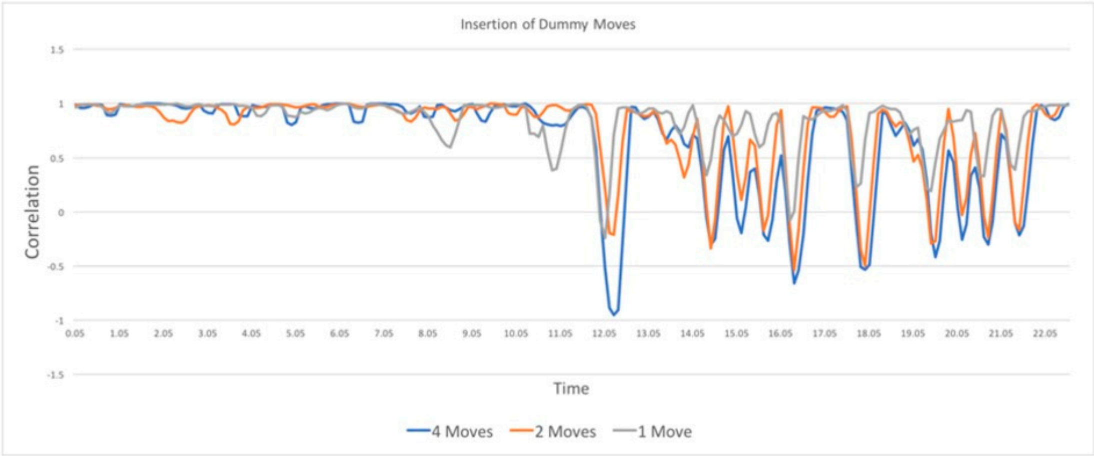



**Figure 8.** Overview of Audio Fingerprint Generation; based on [73].

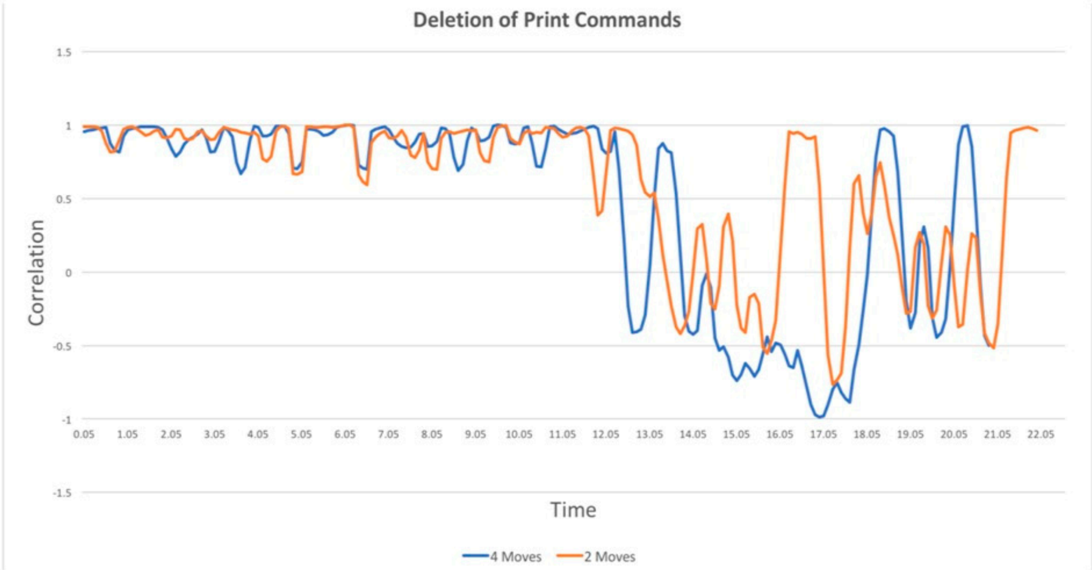
To test these limits, they evaluated various G-code alterations, including Inserting extra G-code, deleting benign G-code, modifying individual movement parameters, changing the extruder speed, and Reordering G-code commands. The results are summarized below in Figure 9.

 doi:10.20944/preprints202506.2516.v1






(a)




(b)

**Figure 9.** Audio Comparison by (a) original cube vs three different cubes (b) original cube vs two different cubes deletion of G1 code; based on the data [73].

Yu et. al [74] discussed the research challenges of designing such a defense system including 1) Accurate modeling and estimation of the status of the AM machine utilizing side-channel information to help one distinguish between ordinary operational faults with tolerances and intrusions and attacks; 2) At the core of this work is the construction of an accurate detection system capable of spotting intrusions and attacks occurring at several phases in the AM digital production chain while following the limits of low-cost sensors, and; 3) designing the system non-intrusive such that it can be implemented with current AM systems. The authors demonstrated vulnerability in critical components, namely Gear and Wrench, emphasizing the need for robust detection systems to prevent structural failures. The proposed system continuously monitored analog side-channel emissions (O) and compared them to inferred control signals (Y) derived from the AM system. The system used supervised ML to establish estimation functions based on the benchmark printer's analog emissions and control signals derived from G-code. Various sensors (current, electromagnetic, vibration, and acoustic) have been utilized to gather emissions, and the system compared real control signals against those estimated by the system. In addition, the system compared real control signals against those estimated by the system.

Zeltmann et. al [71] examined two cyber-physical attack strategies targeting 3D printing: embedding internal defects within printed structures and altering the orientation during the printing

 doi:10.20944/preprints202506.2516.v1



process. These manipulations can compromise structural integrity, leading to weakened products with reduced strength and lower failure strain. Zeltmann's findings indicate that these attacks introduce defects in different locations than those identified by Sturm [69], suggesting variation in attack methodologies and effects on printed components. Moreover, the study revealed that ultrasonic detection, a common non-destructive evaluation technique, struggled to identify both types of alterations effectively. This limitation underscores a significant security vulnerability, as undetected embedded defects and orientation changes could degrade performance in critical applications, potentially leading to premature failure in high-stakes fields such as aerospace, automotive, and medical devices.

Wu and Moon [75] demonstrated a complete cyber-physical attack chain within a manufacturing environment, tracing the process from an initial cyber intrusion to the physical destruction of the target system. In this study, the attack was designed to weaken a 3D-printed drone propeller by subtly altering its structural integrity, ultimately reducing the component's fatigue life. As a result, the compromised propeller failed during flight, underscoring the real-world risks associated with cyber-physical vulnerabilities in manufacturing systems. The findings underscore the potential dangers of cyber-attacks in environments reliant on AM, where even minor digital alterations can lead to significant mechanical failures. This case illustrates how cyber-physical attacks pose tangible threats, particularly in fields that require high reliability, such as aerospace and defense, where compromised components can lead to operational hazards and safety risks.

Above all, the scenario considerations, cyberspace is now vulnerable, and many researchers have proposed various solutions based on different attack scenarios. In the next section, we will discuss the current challenges regarding DTs, including AI integration with cybersecurity considerations.

## 5. Challenges and Possible Solutions

A transformation, including DTs, AI, and cybersecurity, into AM systems creates numerous challenges as well. Solving these problems will help us fully realize the advantages that contemporary technology has to offer.

### *5.1. Cybersecurity Vulnerabilities*

AM systems are particularly prone to cyber-physical attacks since their components—digital and physical ones connected—are vulnerable. Targeting key components, such as STL files, G-code, cloud networks, and AI models, will help mitigate operational downtime, ensure product integrity, and address safety concerns. Although intrusion detection systems are experiencing advancements, identifying minute, process-level changes resulting from attackers remains challenging.

### *5.2. Possible Solutions*

- Shi et al. (2023) proposed using side-channel data—such as acoustic signals and vibrations—in combination with AI-based anomaly detection to increase the accuracy of attack detection and hence support real-time monitoring operations.
- Blockchain technology is recommended for inclusion to create unalterable audit trails for important design files, including STL and G-code. Blockchain technology's distributed ledger enables the verification of manufacturing operations' legality by preventing unauthorized access and ensuring the authenticity of files throughout the production process [76,77].
- Developing advanced encryption techniques in conjunction with blockchain technology will help ensure the security of the transport and storage of design files and sensitive data.

#### 5.2.1. AI-Driven System Reliability

 doi:10.20944/preprints202506.2516.v1



AI models might not function accurately if they are not trained or validated on a range of high-quality datasets. Overstocking AI could lead to errors, especially in cases when input data or feedback loops are defective. The possible solutions are:

- Regularly updating AI models with real-world data helps increase the accuracy of forecasts and flexibility in adapting to changing AM conditions.
- Using blockchain-based smart contracts can help AI become more dependable, as these contracts can automate model modifications and validate the integrity of training data. This ensures that the improvement of models relies solely on approved and objective datasets [78–81].
- Using hybrid decision-making models that combine AI automation with human supervision can ensure that critical operations deliver reliable results.

#### 5.2.2. The Challenge in Combining Physical and Digital Systems

To achieve seamless integration between physical production systems, data transmission systems (DTs), sensors, and AI frameworks, precise calibration is required. The intricacy of this process stems from changes in the material's properties, variations in the surroundings, and equipment limitations. The possible solutions are:

- Wang et al. (2020) have proposed the application of modular AI frameworks that can adjust to unexpected environments, including material discrepancies.
- Traceability solutions by blockchain technology can closely track the whole production process, and this guarantees that the data obtained from sensors, DTs, and AI models is preserved in a safe manner and can be validated, therefore helping with system synchronization and the resolution of any potential errors [82–85].
- Edge computing can enable rapid changes within AM processes and facilitate real-time data processing, thereby helping to minimize the number of delays generated by centralized technology [86].

#### 5.2.3. High Costs and Resource Requirements

Implementing deep learning systems, AI systems, and robust cybersecurity measures requires substantial computational resources and significant financial investment. Regarding small and medium-sized companies eager to use innovative AM technologies, these limitations create significant challenges [87,88]. The possible solutions are:

- Use cloud-based systems to lower starting costs and enable less privileged people to access highly performing technologies [89–91].
- Promote the creation of blockchain-based cooperative networks that enable small and medium-sized businesses to exchange resources and access verified manufacturing data, thereby reducing the cost of individual investments [80,85,92].
- Encouragement of open-source projects and industrial partnerships helps enable the distribution of resources, accelerate development, and lower total costs for stakeholders.

### *5.3. Shortcomings and Proposed Framework*

The increasing challenge of high-quality, traceable, and self-sufficient manufacturing in significant industries such as aerospace, biomedical, and defense has prompted AM to move ahead of traditional layer-by-layer fabrication. Developing challenges involving lack of process comprehensibility, sensitivity to defects, IP theft, and system-level inflexibility now demand the integration of advanced digital technologies. In response, we propose a comprehensive framework that combines Blockchain, Artificial Intelligence (AI), and Digital Twin technologies into an interactive ecosystem, designed to advance the intelligence, security, and self-sufficiency of AM processes.

#### 5.3.1. Framework Overview and Architecture

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2025 doi:10.20944/preprints202506.2516.v1



Figure 10. demonstrates the architecture of the proposed framework. The system is comprised of four core components: (i) a high-reliability digital twin module, (ii) an AI-driven analytics and controller engine, (iii) a blockchain-based distributed network, and (iv) a transposition middleware that permits real-time synchronization and data integrity across subsystems. These components mutually form a closed-loop, intelligent AM self-control system capable of predictive optimization, secure traceability, and combined decision-making.

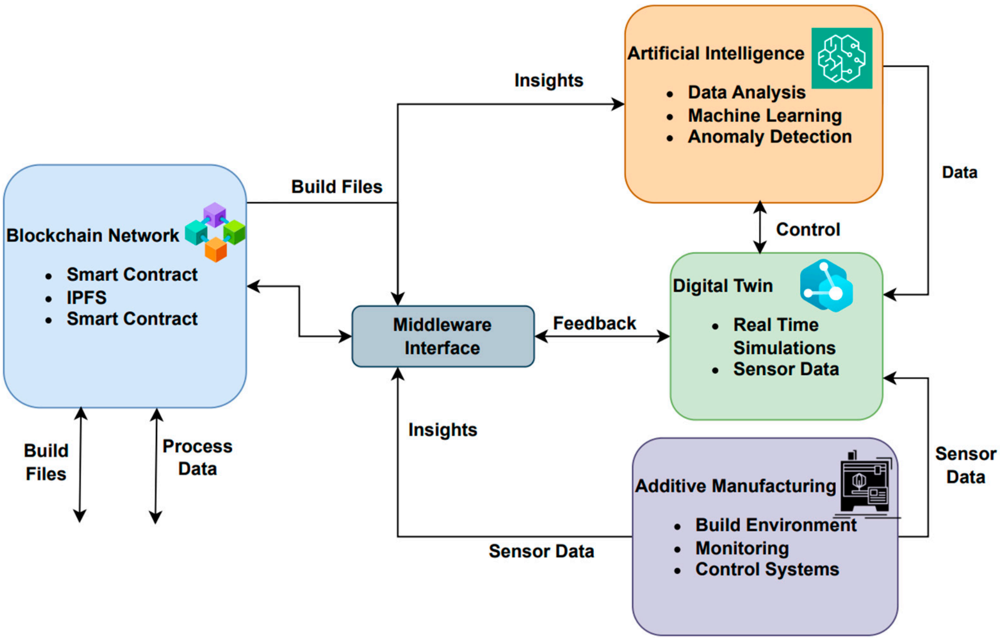



**Figure 10.** Integrating Blockchain, AI, and Digital Twin in AM.

5.3.2. Digital Twin Layer: Real-Time Process Replication and Simulation

The Digital Twin module controls an active, bi-directionally coupled virtual replica of the physical AM system. It reflects the thermal, mechanical, and geometrical development of parts during fabrication by integrating physics-based models with real-time sensor data gathered from the build platform, comprising temperature fields, scan paths, melt pool dimensions, laser energy input, and part distortion [93,94].

The twin supports:

- Real-time checking of in-process abnormalities (e.g., overheating, delamination, recoater failures),
- Predictive simulations handling finite element or reduced-order simulations for thermal and residual stress inference,
- Control validation by evaluating expected results against live sensor feedback.

This digital model also supports virtual commissioning of toolpath approaches, new process parameters, or part designs with no risk to physical hardware, decreasing downtime and cost [95].

5.3.3. AI Layer: Data-Driven Intelligence and Control Optimization

Built on top of the digital twin, the AI layer transforms raw sensor and simulation data into actionable insights. The module incorporates:

- Physics-Informed Neural Networks (PINNs) for explaining inverse problems such as rebuilding indefinite boundary conditions from partial thermal data [96],

- Deep learning models (e.g., CNNs, LSTMs) trained on prior process data to estimate defect formation, porosity zones, or layer-wise quality differences [97],
- Reinforcement Learning (RL) drivers learn to independently adjust laser power, scan speed, or hatch spaces in real time to enhance process results[98].

For example, if the AI detects irregular thermal gradients indicating potential part distortion, it can request the digital twin for simulated effects of parameter variations, identify the optimal solution, and revise the controller all within a single build cycle. This establishes a cyber-physical feedback loop, where the AI continually improves itself through real-world experimentation and simulated scenarios.

5.3.4. Blockchain Layer: Secure Traceability, IP Management, and Smart Contracts

The Blockchain layer tackles two primary concerns in AM: data reliability and intellectual property protection. In this framework, every critical task, such as creating a G-code toolpath, sensor data logging, anomaly detection, or final part authorization, is timestamped and hashed using SHA-256 and logged on a private blockchain network. This ledger:

- Generates a tamper-proof audit trail for build records, parameter changes, and failure events [99],
- Implements access control using smart contracts to guarantee only authorized personnel or collaborators can view/edit critical data [100],
- Enables IP protection by combining design files, toolpaths, and quality metrics to unique blockchain logs, preventing unauthorized access or modifications.

For storage scalability, large datasets (e.g., STL files, thermal maps) are stored on the InterPlanetary File System (IPFS), and only the cryptographic hash is stored on the blockchain. This framework considers immutability in conjunction with performance and confirms the non-repudiation of all manufacturing data in both shared and distributed AM environments.

5.3.5. Middleware Orchestration: Real-Time Integration and Interoperability

At the core of the framework sits the middleware orchestration layer, which delivers the communication interface and synchronization protocols joining the digital twin, AI engine, blockchain, and physical AM machine. This layer controls:

- Event-driven interaction, allowing data triggers (e.g., thermal anomaly detection) to use blockchain transactions or AI-based control updates,
- Standardized data formats and ontologies for inferring sensor feedback, simulation outputs, and blockchain metadata throughout subsystems,
- APIs and microservices for integrating external systems, such as PLM systems, ERP tools, or connected manufacturing networks.

It guarantees low-latency, cyber-physically combined feedback loops, admitting real-time control actions (e.g., modifying scan strategy or deposition speed) centered on insights obtained from predictive simulations or AI inference, while recording all operations securely via smart contracts. Such middleware-aided integration aligns with the Industry 4.0 concept of connected, intelligent systems [101] and confirms the advancement of Cyber-Physical Production Systems (CPPS) as defined by Monostori [102].

## 6. Conclusions

In this paper, the development and progress of DTs and AI over time in AM are discussed, and it is concluded that the integration of DTs, AI, and cybersecurity into AM systems is transforming the industry through process optimization and enhanced decision-making. However, the paper also pointed out that the application of these technologies generates various difficulties, most notably threats to cybersecurity, the difficulty of proper integration with both cyber and physical components, and the significant expenses involved in their implementation. To handle these challenges, one must adopt a comprehensive strategy, which could incorporate new technologies such as blockchain technology to enhance security, AI-based detection systems for reliability, and cloud-based platforms to remove financial barriers. The integration of DTs, AI, cybersecurity, and blockchain technology will lead to a manufacturing ecosystem that is stronger, safer, and more productive. The key points are:

- This paper summarizes and critically analyzes multiple data-driven (DT) architectures for additive manufacturing (AM), including mechanical, control, and machine learning-based models, and discusses their role in in-situ monitoring and process optimization.
- This paper reviews the role of dynamic and modular AI frameworks, including PINNs, CNNs, LSTMs, and RL algorithms, in adjusting real-time AM process parameters, such as laser power and scan speed, to optimize build quality.
- The paper proposes a holistic closed-loop architecture that combines a Digital Twin, AI, a blockchain network, and real-time middleware orchestration to enable intelligent control, predictive process optimization, and secure cyber-physical interaction in additive manufacturing (AM) production systems.

The continuous convergence and development of frameworks for DTs, AI, cybersecurity, and blockchain technologies will cause significant change in the AM sector in the not-too-distant future. The possibility of adaptive manufacturing systems will create chances for new business models, supply chains, and manufacturing processes. It will be imperative to conduct continuous research and development if we are to realize this promise in terms of addressing the technical challenges related to data security and system integration. Establishing industry-wide criteria and open-source projects will be crucial to ensuring that everyone has equitable access to these transformative technologies and, consequently, to foster innovation throughout the sector. Working together, the manufacturing community can propel the next wave of industrial innovation. Unlocking new degrees of efficiency, sustainability, and resilience in AM systems can help one achieve this.

**Author Contributions:** Conceptualization, M.S.A., and M.A.M.; methodology, M.S.A., L.K. and MAM.; software, M.S.A.; validation, M.S.A., L.K. and M.A.M.; formal analysis, M.S.A. and M.A.M.; investigation, M.A.M and F.L.; resources, F.L.; data curation, M.S.A., L.K. and M.A.M.; writing—original draft preparation, M.S.A., L.K. and M.A.M.; writing—review and editing, M.S.A., L.K. and M.A.M. and F.L.; visualization, M.S.A. and L.K..; supervision, F.L.; project administration, F.L.; funding acquisition, F.L. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was partially funded by NSF EEC 1937128, and the Intelligent Systems Center at Missouri University of Science and Technology.

**Data Availability Statement:** No new data was created.

**Conflicts of Interest:** Not applicable.

## Reference

1. Singh, M., Fuenmayor, E., Hinchy, E., Qiao, Y., Murray, N., Devine, D.: Digital Twin: Origin to Future. Applied System Innovation. 4, 36 (2021). https://doi.org/10.3390/asi4020036
2. Armstrong, M., Mehrabi, H., Naveed, N.: An overview of modern metal additive manufacturing technology. J Manuf Process. 84, 1001–1029 (2022). https://doi.org/10.1016/j.jmapro.2022.10.060
3. Fei Tao, Meng Zhang, A.Y.C. Nee: Digital Twin Driven Smart Manufacturing. (2019)
4. Erol, T., Mendi, A.F., Dogan, D.: Digital Transformation Revolution with Digital Twin Technology. In: 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). pp. 1–7. IEEE (2020)

5. Glaessgen, E., Stargel, D.: The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles. In: 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference<BR>20th AIAA/ASME/AHS Adaptive Structures Conference<BR>14th AIAA. American Institute of Aeronautics and Astronautics, Reston, Virigina (2012)
6. Grieves, M.: Back to the Future: Product Lifecycle Management and the Virtualization of Product Information. In: Product Realization. pp. 1–13. Springer US, Boston, MA (2009)
7. Ahn, D.-G.: Directed Energy Deposition (DED) Process: State of the Art. International Journal of Precision Engineering and Manufacturing-Green Technology. 8, 703–742 (2021). https://doi.org/10.1007/s40684-020-00302-7
8. Lim, K.Y.H., Zheng, P., Chen, C.-H.: A state-of-the-art survey of Digital Twin: techniques, engineering product lifecycle management and business innovation perspectives. J Intell Manuf. 31, 1313–1337 (2020). https://doi.org/10.1007/s10845-019-01512-w
9. Zhang, L., Chen, X., Zhou, W., Cheng, T., Chen, L., Guo, Z., Han, B., Lu, L.: Digital Twins for Additive Manufacturing: A State-of-the-Art Review. Applied Sciences. 10, 8350 (2020). https://doi.org/10.3390/app10238350
10. Gaikwad, A., Yavari, R., Montazeri, M., Cole, K., Bian, L., Rao, P.: Toward the digital twin of additive manufacturing: Integrating thermal simulations, sensing, and analytics to detect process faults. IISE Trans. 52, 1204–1217 (2020). https://doi.org/10.1080/24725854.2019.1701753
11. Liu, C., Le Roux, L., Körner, C., Tabaste, O., Lacan, F., Bigot, S.: Digital Twin-enabled Collaborative Data Management for Metal Additive Manufacturing Systems. J Manuf Syst. 62, 857–874 (2022). https://doi.org/10.1016/j.jmsy.2020.05.010
12. Sujit Rokka Chhetri, Sina Faezi, Mohammad Abdullah Al Faruque: Digital Twin of Manufacturing Systems. , Irvine Irvine, CA 92697-2620, USA (2017)
13. Knapp, G.L., Mukherjee, T., Zuback, J.S., Wei, H.L., Palmer, T.A., De, A., DebRoy, T.: Building blocks for a digital twin of additive manufacturing. Acta Mater. 135, 390–399 (2017). https://doi.org/10.1016/j.actamat.2017.06.039
14. DebRoy, T., Zhang, W., Turner, J., Babu, S.S.: Building digital twins of 3D printing machines. Scr Mater. 135, 119–124 (2017). https://doi.org/10.1016/j.scriptamat.2016.12.005
15. Choudhary, A., Chaudhary, A., Devi, S.: Cyber Security With Emerging Technologies & Challenges. In: 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N). pp. 1875–1879. IEEE (2022)
16. Hossain Faruk, M.J., Tahora, S., Tasnim, M., Shahriar, H., Sakib, N.: A Review of Quantum Cybersecurity: Threats, Risks and Opportunities. In: 2022 1st International Conference on AI in Cybersecurity (ICAIC). pp. 1–8. IEEE (2022)
17. Rajasekharaiah, K.M., Dule, C.S., Sudarshan, E.: Cyber Security Challenges and its Emerging Trends on Latest Technologies. IOP Conf Ser Mater Sci Eng. 981, 022062 (2020). https://doi.org/10.1088/1757-899X/981/2/022062
18. Mukherjee, T., DebRoy, T.: A digital twin for rapid qualification of 3D printed metallic components. Appl Mater Today. 14, 59–65 (2019). https://doi.org/10.1016/j.apmt.2018.11.003
19. Thejane, K., du Preez, W., Booysen, G.: Implementing digital twinning in an additive manufacturing process chain. MATEC Web of Conferences. 388, 10001 (2023). https://doi.org/10.1051/matecconf/202338810001
20. Phanden, R.K., Aditya, S.V., Sheokand, A., Goyal, K.K., Gahlot, P., Jacso, A.: A state-of-the-art review on implementation of digital twin in additive manufacturing to monitor and control parts quality. Mater Today Proc. 56, 88–93 (2022). https://doi.org/10.1016/j.matpr.2021.12.217
21. Chen, L., Bi, G., Yao, X., Tan, C., Su, J., Ng, N.P.H., Chew, Y., Liu, K., Moon, S.K.: Multisensor fusion-based digital twin for localized quality prediction in robotic laser-directed energy deposition. Robot Comput Integr Manuf. 84, 102581 (2023). https://doi.org/10.1016/j.rcim.2023.102581
22. Xu, S., Lu, Y., Yu, C.: Augmented reality-assisted cloud additive manufacturing with digital twin technology for multi-stakeholder value Co-creation in product innovation. Heliyon. 10, e25722 (2024). https://doi.org/10.1016/j.heliyon.2024.e25722

23. Phua, A., Davies, C.H.J., Delaney, G.W.: A digital twin hierarchy for metal additive manufacturing. Comput Ind. 140, 103667 (2022). https://doi.org/10.1016/j.compind.2022.103667
24. Kanthimathi, T., Rathika, N., Fathima, A.J., K S, R., Srinivasan, S., R, T.: Robotic 3D Printing for Customized Industrial Components: IoT and AI-Enabled Innovation. In: 2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence). pp. 509–513. IEEE (2024)
25. Yin Z, H., Wang, L.: Application and Development Prospect of Digital Twin Technology in Aerospace. IFAC-PapersOnLine. 53, 732–737 (2020). https://doi.org/10.1016/j.ifacol.2021.04.165
26. Jin, L., Zhai, X., Wang, K., Zhang, K., Wu, D., Nazir, A., Jiang, J., Liao, W.-H.: Big data, machine learning, and digital twin assisted additive manufacturing: A review. Mater Des. 244, 113086 (2024). https://doi.org/10.1016/j.matdes.2024.113086
27. Chen, L., Yao, X., Liu, K., Tan, C., Moon, S.K.: MULTISENSOR FUSION-BASED DIGITAL TWIN IN ADDITIVE MANUFACTURING FOR IN-SITU QUALITY MONITORING AND DEFECT CORRECTION. Proceedings of the Design Society. 3, 2755–2764 (2023). https://doi.org/10.1017/pds.2023.276
28. Jannesari Ladani, L.: Applications of artificial intelligence and machine learning in metal additive manufacturing. Journal of Physics: Materials. 4, 042009 (2021). https://doi.org/10.1088/2515-7639/ac2791
29. Aziz, N.A., Adnan, N.A.A., Wahab, D.A., Azman, A.H.: Component design optimisation based on artificial intelligence in support of additive manufacturing repair and restoration: Current status and future outlook for remanufacturing. J Clean Prod. 296, 126401 (2021). https://doi.org/10.1016/j.jclepro.2021.126401
30. He, F., Yuan, L., Mu, H., Ros, M., Ding, D., Pan, Z., Li, H.: Research and application of artificial intelligence techniques for wire arc additive manufacturing: a state-of-the-art review. Robot Comput Integr Manuf. 82, 102525 (2023). https://doi.org/10.1016/j.rcim.2023.102525
31. Arinez, J.F., Chang, Q., Gao, R.X., Xu, C., Zhang, J.: Artificial Intelligence in Advanced Manufacturing: Current Status and Future Outlook. J Manuf Sci Eng. 142, (2020). https://doi.org/10.1115/1.4047855
32. Çınar, Z.M., Abdussalam Nuhu, A., Zeeshan, Q., Korhan, O., Asmael, M., Safaei, B.: Machine Learning in Predictive Maintenance towards Sustainable Smart Manufacturing in Industry 4.0. Sustainability. 12, 8211 (2020). https://doi.org/10.3390/su12198211
33. Soori, M., Arezoo, B., Dastres, R.: Artificial intelligence, machine learning and deep learning in advanced robotics, a review. Cognitive Robotics. 3, 54–70 (2023). https://doi.org/10.1016/j.cogr.2023.04.001
34. Wang, C., Tan, X.P., Tor, S.B., Lim, C.S.: Machine learning in additive manufacturing: State-of-the-art and perspectives. Addit Manuf. 36, 101538 (2020). https://doi.org/10.1016/j.addma.2020.101538
35. Guo, K., Yang, Z., Yu, C.-H., Buehler, M.J.: Artificial intelligence and machine learning in design of mechanical materials. Mater Horiz. 8, 1153–1172 (2021). https://doi.org/10.1039/D0MH01451F
36. Qin, J., Hu, F., Liu, Y., Witherell, P., Wang, C.C.L., Rosen, D.W., Simpson, T.W., Lu, Y., Tang, Q.: Research and application of machine learning for additive manufacturing. Addit Manuf. 52, 102691 (2022). https://doi.org/10.1016/j.addma.2022.102691
37. Dipak Kumar Banerjee, Ashok Kumar, K.S.: Artificial Intelligence on Additive Manufacturing. International IT Journal of Research. 02, 02 (2024)
38. Wang, Y., Zheng, P., Peng, T., Yang, H., Zou, J.: Smart additive manufacturing: Current artificial intelligence-enabled methods and future perspectives. Sci China Technol Sci. 63, 1600–1611 (2020). https://doi.org/10.1007/s11431-020-1581-2
39. Masinelli, G., Shevchik, S.A., Pandiyan, V., Quang-Le, T., Wasmer, K.: Artificial Intelligence for Monitoring and Control of Metal Additive Manufacturing. In: Industrializing Additive Manufacturing. pp. 205–220. Springer International Publishing, Cham (2021)
40. Heiden, B., Alieksieiev, V., Volk, M., Tonino-Heiden, B.: Framing Artificial Intelligence (AI) Additive Manufacturing (AM). Procedia Comput Sci. 186, 387–394 (2021). https://doi.org/10.1016/j.procs.2021.04.161
41. Jin, Z., Zhang, Z., Gu, G.X.: Automated Real-Time Detection and Prediction of Interlayer Imperfections in Additive Manufacturing Processes Using Artificial Intelligence. Advanced Intelligent Systems. 2, (2020). https://doi.org/10.1002/aisy.201900130
42. Elambasseril, J., Brandt, M.: Artificial intelligence: way forward to empower metal additive manufacturing product development – an overview. Mater Today Proc. 58, 461–465 (2022). https://doi.org/10.1016/j.matpr.2022.02.485

43. Gu, S., Choi, M., Park, H., Jeong, S., Doh, J., Park, S.: Application of artificial intelligence in additive manufacturing. JMST Advances. 5, 93–104 (2023). https://doi.org/10.1007/s42791-023-00057-7
44. Johnson, M. V., Garanger, K., Hardin, J.O., Berrigan, J.D., Feron, E., Kalidindi, S.R.: A generalizable artificial intelligence tool for identification and correction of self-supporting structures in additive manufacturing processes. Addit Manuf. 46, 102191 (2021). https://doi.org/10.1016/j.addma.2021.102191
45. Choi, W., Advincula, R.C., Wu, H.F., Jiang, Y.: Artificial intelligence and machine learning in the design and additive manufacturing of responsive composites. MRS Commun. 13, 714–724 (2023). https://doi.org/10.1557/s43579-023-00473-9
46. Hartmann, S., Vykhtar, B., Möbs, N., Kelbassa, I., Mayr, P.: IoT-Based Data Mining Framework for Stability Assessment of the Laser-Directed Energy Deposition Process. Processes. 12, 1180 (2024). https://doi.org/10.3390/pr12061180
47. Ahmadi, F., Song, J., Zoughi, R.: Electromagnetic Scattering Properties of Metal Powder Cloud for Laser Powder Bed Fusion (LPBF) Additive Manufacturing (AM). IEEE Open Journal of Antennas and Propagation. 1–1 (2024). https://doi.org/10.1109/OJAP.2024.3431536
48. Zhu, Q., Liu, Z., Yan, J.: Machine learning for metal additive manufacturing: predicting temperature and melt pool fluid dynamics using physics-informed neural networks. Comput Mech. 67, 619–635 (2021). https://doi.org/10.1007/s00466-020-01952-9
49. Meng, L., McWilliams, B., Jarosinski, W., Park, H.-Y., Jung, Y.-G., Lee, J., Zhang, J.: Machine Learning in Additive Manufacturing: A Review. JOM. 72, 2363–2377 (2020). https://doi.org/10.1007/s11837-020-04155-y
50. Goh, G.D., Sing, S.L., Yeong, W.Y.: A review on machine learning in 3D printing: applications, potential, and challenges. Artif Intell Rev. 54, 63–94 (2021). https://doi.org/10.1007/s10462-020-09876-9
51. Wang, C., Tan, X.P., Tor, S.B., Lim, C.S.: Machine learning in additive manufacturing: State-of-the-art and perspectives. Addit Manuf. 36, 101538 (2020). https://doi.org/10.1016/j.addma.2020.101538
52. Throne, O., Lăzăroiu, G.: Internet of Things-enabled Sustainability, Industrial Big Data Analytics, and Deep Learning-assisted Smart Process Planning in Cyber-Physical Manufacturing Systems. Economics, Management, and Financial Markets. 15, 49 (2020). https://doi.org/10.22381/EMFM15420205
53. Andronie, M., Lăzăroiu, G., Ștefănescu, R., Uță, C., Dijmărescu, I.: Sustainable, Smart, and Sensing Technologies for Cyber-Physical Manufacturing Systems: A Systematic Literature Review. Sustainability. 13, 5495 (2021). https://doi.org/10.3390/su13105495
54. Nguyen, T.N., Zeadally, S., Vuduthala, A.B.: Cyber-Physical Cloud Manufacturing Systems With Digital Twins. IEEE Internet Comput. 26, 15–21 (2022). https://doi.org/10.1109/MIC.2021.3058921
55. Balta, E.C., Pease, M., Moyne, J., Barton, K., Tilbury, D.M.: Digital Twin-Based Cyber-Attack Detection Framework for Cyber-Physical Manufacturing Systems. IEEE Transactions on Automation Science and Engineering. 21, 1695–1712 (2024). https://doi.org/10.1109/TASE.2023.3243147
56. Wu, Y., Cao, H., Yang, G., Lu, T., Wan, S.: Digital Twin of Intelligent Small Surface Defect Detection with Cyber-manufacturing Systems. ACM Trans Internet Technol. 23, 1–20 (2023). https://doi.org/10.1145/3571734
57. Dafflon, B., Moalla, N., Ouzrout, Y.: The challenges, approaches, and used techniques of CPS for manufacturing in Industry 4.0: a literature review. The International Journal of Advanced Manufacturing Technology. 113, 2395–2412 (2021). https://doi.org/10.1007/s00170-020-06572-4
58. Corallo, A., Lazoi, M., Lezzi, M., Pontrandolfo, P.: Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level. IEEE Trans Eng Manag. 70, 3745–3765 (2023). https://doi.org/10.1109/TEM.2021.3084687
59. Wu, M., Song, Z., Moon, Y.B.: Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods. J Intell Manuf. 30, 1111–1123 (2019). https://doi.org/10.1007/s10845-017-1315-5
60. Yampolskiy, M., Horvath, P., Koutsoukos, X.D., Xue, Y., Sztipanovits, J.: Taxonomy for description of cross-domain attacks on CPS. In: Proceedings of the 2nd ACM international conference on High confidence networked systems. pp. 135–142. ACM, New York, NY, USA (2013)
61. Wu, M., Moon, Y.B.: Taxonomy for Secure CyberManufacturing Systems. In: Volume 2: Advanced Manufacturing. American Society of Mechanical Engineers (2018)

62. Dave, M.: Internet of Things Security and Forensics: Concern and Challenges for Inspecting Cyber Attacks. In: 2022 Second International Conference on Next Generation Intelligent Systems (ICNGIS). pp. 1–6. IEEE (2022)
63. Wang, L., Mosher, R.L., Duett, P.: Cyberattacks and Cybersecurity in Additive Manufacturing. In: SoutheastCon 2024. pp. 1040–1045. IEEE (2024)
64. Mahan, T., Menold, J.: Simulating cyber-physical systems: Identifying vulnerabilities for design and manufacturing through simulated additive manufacturing environments. Addit Manuf. 35, 101232 (2020). https://doi.org/10.1016/j.addma.2020.101232
65. Mullet, V., Sondi, P., Ramat, E.: A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0. IEEE Access. 9, 23235–23263 (2021). https://doi.org/10.1109/ACCESS.2021.3056650
66. Raza, A., Memon, S., Nizamani, M.A., Hussain Shah, M.: Machine Learning-Based Security Solutions for Critical Cyber-Physical Systems. In: 2022 10th International Symposium on Digital Forensics and Security (ISDFS). pp. 1–6. IEEE (2022)
67. Torbacki, W.: A Hybrid MCDM Model Combining DANP and PROMETHEE II Methods for the Assessment of Cybersecurity in Industry 4.0. Sustainability. 13, 8833 (2021). https://doi.org/10.3390/su13168833
68. Daim, T., Yalcin, H., Mermoud, A., Mulder, V.: Exploring cybertechnology standards through bibliometrics: Case of National Institute of Standards and Technology. World Patent Information. 77, 102278 (2024). https://doi.org/10.1016/j.wpi.2024.102278
69. Sturm, L.D., Williams, C.B., Camelio, J.A., White, J., Parker, R.: Cyber-Physical Vulnerabilities in Additive Manufacturing Systems. Presented at the (2014)
70. Turner, H., White, J., Camelio, J.A., Williams, C., Amos, B., Parker, R.: Bad Parts: Are Our Manufacturing Systems at Risk of Silent Cyberattacks? IEEE Secur Priv. 13, 40–47 (2015). https://doi.org/10.1109/MSP.2015.60
71. Zeltmann, S.E., Gupta, N., Tsoutsos, N.G., Maniatakos, M., Rajendran, J., Karri, R.: Manufacturing and Security Challenges in 3D Printing. JOM. 68, 1872–1881 (2016). https://doi.org/10.1007/s11837-016-1937-7
72. Shi, Z., Mamun, A. Al, Kan, C., Tian, W., Liu, C.: An LSTM-autoencoder based online side channel monitoring approach for cyber-physical attack detection in additive manufacturing. J Intell Manuf. 34, 1815–1831 (2023). https://doi.org/10.1007/s10845-021-01879-9
73. Sofia Belikovetsky, Yosef Solewicz, Mark Yampolskiy, Jinghui Toh, Yuval Elovici: Detecting Cyber-Physical Attacks in Additive Manufacturing using Digital Audio Signing. (2017)
74. Yu, S.-Y., Malawade, A.V., Chhetri, S.R., Al Faruque, M.A.: Sabotage Attack Detection for Additive Manufacturing Systems. IEEE Access. 8, 27218–27231 (2020). https://doi.org/10.1109/ACCESS.2020.2971947
75. Wu, M., Moon, Y.B.: Intrusion Detection of Cyber-Physical Attacks in Manufacturing Systems: A Review. In: Volume 2B: Advanced Manufacturing. American Society of Mechanical Engineers (2019)
76. Haridas, A., Samad, A.A., D, V., K, D.L., Pathari, V.: A blockchain-based platform for smart contracts and intellectual property protection for the additive manufacturing industry. In: 2022 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES). pp. 223–230. IEEE (2022)
77. Shi, Z., Kan, C., Tian, W., Liu, C.: A Blockchain-Based G-Code Protection Approach for Cyber-Physical Security in Additive Manufacturing. J Comput Inf Sci Eng. 21, (2021). https://doi.org/10.1115/1.4048966
78. Haw, J., Dola, T.A., Sing, S.L., Tan, E.Y.S., Liu, A.Z.: Blockchain for Additive Manufacturing. In: Additive Manufacturing Design and Applications. pp. 582–587. ASM International (2023)
79. Westphal, E., Leiding, B., Seitz, H.: Blockchain-based quality management for a digital additive manufacturing part record. J Ind Inf Integr. 35, 100517 (2023). https://doi.org/10.1016/j.jii.2023.100517
80. Lupi, F., Cimino, M.G.C.A., Berlec, T., Galatolo, F.A., Corn, M., Rožman, N., Rossi, A., Lanzetta, M.: Blockchain-based Shared Additive Manufacturing. Comput Ind Eng. 183, 109497 (2023). https://doi.org/10.1016/j.cie.2023.109497
81. Alkhader, W., Alkaabi, N., Salah, K., Jayaraman, R., Arshad, J., Omar, M.: Blockchain-Based Traceability and Management for Additive Manufacturing. IEEE Access. 8, 188363–188377 (2020). https://doi.org/10.1109/ACCESS.2020.3031536

82. Guo, D., Ling, S., Li, H., Ao, D., Zhang, T., Rong, Y., Huang, G.Q.: A framework for personalized production based on digital twin, blockchain and additive manufacturing in the context of Industry 4.0. In: 2020 IEEE 16th International Conference on Automation Science and Engineering (CASE). pp. 1181–1186. IEEE (2020)
83. Ghimire, T., Joshi, A., Sen, S., Kapruan, C., Chadha, U., Selvaraj, S.K.: Blockchain in additive manufacturing processes: Recent trends & its future possibilities. Mater Today Proc. 50, 2170–2180 (2022). https://doi.org/10.1016/j.matpr.2021.09.444
84. Chadha, U., Abrol, A., Vora, N.P., Tiwari, A., Shanker, S.K., Selvaraj, S.K.: Performance evaluation of 3D printing technologies: a review, recent advances, current challenges, and future directions. Progress in Additive Manufacturing. 7, 853–886 (2022). https://doi.org/10.1007/s40964-021-00257-4
85. Kurpjuweit, S., Schmidt, C.G., Klöckner, M., Wagner, S.M.: Blockchain in Additive Manufacturing and its Impact on Supply Chains. Journal of Business Logistics. 42, 46–70 (2021). https://doi.org/10.1111/jbl.12231
86. Nain, G., Pattanaik, K.K., Sharma, G.K.: Towards edge computing in intelligent manufacturing: Past, present and future. J Manuf Syst. 62, 588–611 (2022). https://doi.org/10.1016/j.jmsy.2022.01.010
87. Sæterbø, M., Arnarson, H., Yu, H., Solvang, W.D.: Expanding the horizons of metal additive manufacturing: A comprehensive multi-objective optimization model incorporating sustainability for SMEs. J Manuf Syst. 77, 62–77 (2024). https://doi.org/10.1016/j.jmsy.2024.08.026
88. Haug, A., Wickstrøm, K.A., Stentoft, J., Philipsen, K.: Adoption of additive manufacturing: A survey of the role of knowledge networks and maturity in small and medium-sized Danish production firms. Int J Prod Econ. 255, 108714 (2023). https://doi.org/10.1016/j.ijpe.2022.108714
89. Simeone, A., Caggiano, A., Zeng, Y.: Smart cloud manufacturing platform for resource efficiency improvement of additive manufacturing services. Procedia CIRP. 88, 387–392 (2020). https://doi.org/10.1016/j.procir.2020.05.067
90. Rahman, M.A., Shakur, M.S., Ahamed, Md.S., Hasan, S., Rashid, A.A., Islam, M.A., Haque, Md.S.S., Ahmed, A.: A Cloud-Based Cyber-Physical System with Industry 4.0: Remote and Digitized Additive Manufacturing. Automation. 3, 400–425 (2022). https://doi.org/10.3390/automation3030021
91. Haghnegahdar, L., Joshi, S.S., Dahotre, N.B.: From IoT-based cloud manufacturing approach to intelligent additive manufacturing: industrial Internet of Things—an overview. The International Journal of Advanced Manufacturing Technology. 119, 1461–1478 (2022). https://doi.org/10.1007/s00170-021-08436-x
92. Shukla, S., KC, S.: Leveraging Blockchain for sustainability and supply chain resilience in e-commerce channels for additive manufacturing: A cognitive analytics management framework-based assessment. Comput Ind Eng. 176, 108995 (2023). https://doi.org/10.1016/j.cie.2023.108995
93. Tao, F., Zhang, H., Liu, A., Nee, A.Y.C.: Digital Twin in Industry: State-of-the-Art. IEEE Trans Industr Inform. 15, 2405–2415 (2019). https://doi.org/10.1109/TII.2018.2873186
94. Qi, Q., Tao, F.: Digital Twin and Big Data Towards Smart Manufacturing and Industry 4.0: 360 Degree Comparison. IEEE Access. 6, 3585–3593 (2018). https://doi.org/10.1109/ACCESS.2018.2793265
95. Leng, J., Zhang, H., Yan, D., Liu, Q., Chen, X., Zhang, D.: Digital twin-driven manufacturing cyber-physical system for parallel controlling of smart workshop. J Ambient Intell Humaniz Comput. 10, 1155–1166 (2019). https://doi.org/10.1007/s12652-018-0881-5
96. Raissi, M., Perdikaris, P., Karniadakis, G.E.: Physics-informed neural networks: A deep learning framework for solving forward and inverse problems involving nonlinear partial differential equations. J Comput Phys. 378, 686–707 (2019). https://doi.org/10.1016/j.jcp.2018.10.045
97. Equbal, M.A., Equbal, A., Khan, Z.A., Badruddin, I.A.: Machine learning in additive manufacturing: A comprehensive insight. International Journal of Lightweight Materials and Manufacture. 8, 264–284 (2025). https://doi.org/10.1016/j.ijlmm.2024.10.002
98. Li, C., Zheng, P., Yin, Y., Wang, B., Wang, L.: Deep reinforcement learning in smart manufacturing: A review and prospects. CIRP J Manuf Sci Technol. 40, 75–101 (2023). https://doi.org/10.1016/j.cirpj.2022.11.003
99. Alkhader, W., Alkaabi, N., Salah, K., Jayaraman, R., Arshad, J., Omar, M.: Blockchain-Based Traceability and Management for Additive Manufacturing. IEEE Access. 8, 188363–188377 (2020). https://doi.org/10.1109/ACCESS.2020.3031536

doi:10.20944/preprints202506.2516.v1



100. Christidis, K., Devetsikiotis, M.: Blockchains and Smart Contracts for the Internet of Things. IEEE Access. 4, 2292–2303 (2016). https://doi.org/10.1109/ACCESS.2016.2566339
101. Lu, Y.: Industry 4.0: A survey on technologies, applications and open research issues. J Ind Inf Integr. 6, 1–10 (2017). https://doi.org/10.1016/j.jii.2017.04.005
102. Monostori, L.: Cyber-physical Production Systems: Roots, Expectations and R&D Challenges. Procedia CIRP. 17, 9–13 (2014). https://doi.org/10.1016/j.procir.2014.03.115