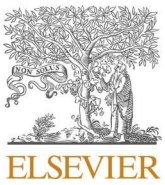
Bioprinting 36 (2023) e00321



Contents lists available at ScienceDirect

Bioprinting

journal homepage: www.sciencedirect.com/journal/bioprinting

# Cybersecurity and privacy in smart bioprinting

Joan C. Isichei[a,c], Sajad Khorsandroo[b,c], Salil Desai[a,c,*]

[a] Department of Industrial and Systems Engineering, 1601 E Market Street, Greensboro, NC, 27401, USA
[b] Department of Computer Science, North Carolina A&T State University, Greensboro, NC, 27411, USA
[c] Center of Excellence in Product Design and Advanced Manufacturing, North Carolina A&T State University, 1601 E Market Street, Greensboro, NC, 27401, USA

ARTI CLE I NFO

Index Terms:
3D printing
Artificial intelligence
Bioprinting
Cybersecurity
Digital twin (DT)
Internet of things (IoT)

ABSTRACT

Bioprinting is a versatile technology gaining rapid adoption in healthcare fields such as tissue engineer regenerative medicine, drug delivery, and surgical planning. Although the current state of the technology is in i infancy, it is envisioned that its evolution will be enabled by the integration of the following technolog Internet of Things (IoT), Cloud computing, Artificial Intelligence/Machine Learning (AI/ML), NextGen Networks, and Blockchain. The product of this integration will eventually be a smart bioprinting ecosystem. This paper presents the smart bioprinting ecosystem as a multilayered architecture and reviews the cyber security chal- lenges, vulnerabilities, and threats in every layer. Furthermore, the paper presents privacy preservation solutio and provides a purview of the open research challenges in the smart bioprinting ecosystem.

## 1. Introduction

In recent times, the spotlight has been cast on advances in bio- printing technology. The primary advantage of bioprinting technology stems from its ability to overcome engineering challenges endemic to tissue engineering [1,2], regenerative medicine [3], drug delivery [4], and surgical planning [5]. Bioprinting can create complex tissue scaf- folds [6,7], implants, patient-specific geometries and devices [8]. Bio- printing entails the detailed layer-by-layer positioning of biocompatible materials, biochemicals, living cells, and other supporting elements for building complex 3D functional living tissues [9]. Attempts have been made using bioprinting technologies to construct tissues such as bone, skin, cartilage, and other complicated tissues such as vasculature and human-scale ear cartilage. Bioprinting includes the use of the following methodologies: "biomimicry, autonomous self-assembly and mini-tissue building blocks" [2,10–13] for the construction of functional living human-like organs. The following section delves into the leading bio- printing technologies, the primary targeted tissues, and this field's remarkable possibilities.

### 1.1. An overview of bioprinting: technologies, challenges, and future

Bioprinting is an emerging technology that has the potential to revolutionize regenerative medicine, providing new ways to treat and repair damaged or diseased tissues and organs. It could also create new drug discovery and toxicology testing models. Bioprinting combines 3D print- ing concepts with biological materials in a complex process that involves the precise deposition of cells and biomaterials to construct structures that mimic the natural functions of tissues and organs. Numerous medical challenges can be addressed by using this innovative approach, such as organ transplantation shortages, tissue repair, and personalized medicine. In bioprinting, the most common target tissues and organs include: 1) Bones and cartilage, 2) Heart, Kidney, and Liver Organs, 3) Vascular Tissues, and 4) Skin and Soft Tissues. Despite its growing popularity, bioprinting is still a relatively new technology, and it faces many challenges before widespread adoption. One major chal- lenge is developing bioprinters that print tissues and organs at hig speeds and precision. Reproducing the incredibly complex micro- architecture and functionality of these organs is an arduous task. Cell viability is another challenge: During and after printing, it is essential to ensure that cells remain viable and functional. Immunological compat- ibility is another challenge: Transplanted bioprinted tissues or organs must not trigger immune responses. Lastly, navigating regulatory pathways and developing standardized procedures are crucial to th mainstream adoption of bioprinting. Given the complexity of working with cells and biomaterials, bioprinting technology is still in its infancy. However, it is envisaged that with the advent of artificial intelligence/ machine learning (AI/ML) algorithms, IoT sensors, cloud computing,

* Corresponding author. Center of Excellence in Product Design and Advanced Manufacturing, North Carolina A &T State University, 1601 E. Market Street, Greensboro, NC, 27401, USA.
E-mail address: sdesai@ncat.edu (S. Desai).

https://doi.org/10.1016/j.bprint.2023.e00321
Received 5 July 2023; Received in revised form 17 October 2023; Accepted 30 October 2023
Available online 31 October 2023

next generation (NextGen) networks, and blockchain technology, a smart bioprinting ecosystem or smart biomanufacturing system would emerge in the near future. It is also envisioned that this ecosystem would help solve the multiscale challenges of current bioprinting processes and applications. A brief overview of machine learning is presented in section 1.2.

#### 1.1.1. Bioprinting Technologies

There are three major bioprinting techniques available, including extrusion-based, inkjet, and laser-assisted bioprinting. They are described as follows.

##### 1.1.1.1. Extrusion based bioprinting

In extrusion-based bioprinting (EBB), bioink is precisely deposited layer-by-layer, ultimately transforming into complex tissue structures using a syringe-like mechanism [14]. The bioink materials used in EBB are primarily viscous hydrogels, with or without cells, that are extruded through nozzles, pneumatically or mechanically, onto substrates. Extrusion-based bioprinters are known for their ability to handle high-viscosity materials and incorporate multiple cell types, allowing for heterogeneous tissue constructs. The technique is essential for tissue engineering, regenerative medicine, and drug testing as it offers the potential to generate functional tissues and organoids similar to their natural counterparts. A wide range of bioprinting applications can be addressed using this approach because of its versatility and adaptability. However, precise control of printing parameters, cell viability, and tissue quality is essential for successful extrusion-based bioprinting applications.

##### 1.1.1.2. Inkjet bioprinting

Like traditional inkjet printing, the principle behind 3D inkjet bioprinting involves depositing bioinks (biological materials) in droplets to form 2D or 3D biological structures using piezoelectricity or a heating strategy. It is commonly used for printing tissues with complex vascular networks [7]. A critical component of 3D inkjet bioprinting is investigating how the combination of individual ink drops occurs. Since the dimension of printable droplets is tiny, bioprinting of a large structure like an organ may prove challenging; however, since the droplet size is miniscule, printing designs of high quality will be achievable. Moreover, in-situ deposition of biochemical growth-factors within pre-extruded biostructures can promote differentiation of specific cell lineages for complex tissue constructs.

##### 1.1.1.3. Laser-assisted bioprinting

In laser-assisted bioprinting (LAB), bioinks are deposited onto a substrate using laser energy. This method offers exceptional control and precision in the placement of cells and biomaterials. In laser-assisted bioprinting, a laser is focused on a ribbon containing the bioink material. When the laser strikes the material, the energy created by the laser beam creates a “cavitation” that propels a cell-containing droplet onto the receiving substrate [15]. LAB is particularly effective for printing delicate cell types and creating complex tissue structures with high resolution. Its ability to maintain cell viability and deposit biomaterials precisely makes it a suitable candidate for tissue engineering, regenerative medicine, and the development of organ-on-a-chip models for drug testing and disease research.

### 1.2. Artificial Intelligence/Machine Learning

Machine learning is one of the fastest-growing technical fields today. As a subset of artificial intelligence, it is a diverse approach focusing primarily on designing algorithms using training, validation, and test datasets that can make predictions, decisions, or actions without explicit programming. Additionally, a cost function is used to determine the effectiveness of the ML model by comparing predicted values to actual values. Optimal model parameters are determined by finding the minima of the cost functions using the optimization algorithms in the cost function. In optimizing bioprinting parameters, a set of prioritized criteria and constraints may be considered to achieve the best printing environment. ML algorithms can provide insight into the complexities of biological systems and enable the extraction of new biological knowledge from complex bioprinting experimental data. It is expected that ML will bring the smart and intelligent bioprinting ecosystem much closer to reality. Based on the signals and feedback the ML algorithm receives, there are three standard machine learning methodologies: supervised ML, unsupervised ML, and reinforcement ML [15]. The following paragraphs provide a detailed description of each machine-learning method.

#### 1.2.1. Supervised machine learning

Supervised learning involves training the algorithm using a labeled dataset consisting of input features and their associated target values. In order for the algorithm to make accurate predictions based on new data, it must learn a mapping between inputs and outputs. The parameters for bioprinting can be optimized through supervised learning. Researchers can create labeled datasets incorporating various bioprinting parameters (e.g., nozzle size, printing speed, temperature, pressure) and corresponding outcomes (e.g., tissue quality, cell viability, structural integrity). The use of these data to train ML models can help predict optimal printing parameters and reduce the number of trials and errors associated with achieving desired tissue properties. The most commonly used supervised ML algorithms include linear regression, logistic regression, decision trees, support vector machines, and neural networks.

#### 1.2.2. Unsupervised machine learning

In unsupervised learning, target labels are not explicitly defined for the dataset. Instead, the algorithm finds patterns, structures, and relationships in the data. In particular, it automatically learns, and extracts features from input data and divides them into clusters. It is the best approach for identifying hidden patterns or relationships within data. In bioprinting, unsupervised learning can group similar data points together, helping researchers identify meaningful patterns and subtypes within their datasets. For instance, it can distinguish between healthy and diseased tissues or classify tissues according to their developmental stage. Unsupervised learning techniques include 1) clustering methods (e.g., K-Means, hierarchical clustering) that group similar data points together and 2) dimensionality reduction methods (e.g., PCA, t-SNE) that simplify complex data.

#### 1.2.3. Reinforcement learning

A reinforcement learning approach involves teaching agents how to interact with an environment in order to maximize their cumulative rewards by learning the optimal actions to take. In bioprinting, tissues are built up layer-by-layer. The RL algorithm can optimize various parameters for each layer, such as bioink type, printing speed, temperature, and pressure. These parameters can be adjusted by RL agents based on feedback to improve tissue quality. Q-Learning, Deep Q-Networks (DQN), and policy gradient methods are some of the most common RL algorithms.

### 1.3. Application of AI/ML in bioprinting

The application of artificial intelligence to bioprinting is increasingly becoming more common as a way to enhance its capabilities and address complex challenges. Ruberu et al. [16], investigated the feasibility of using machine learning to optimize the printability of extrusion printing of GelMA and GelMA/HAMA bioinks to achieve a reproducible 3D print with good shape fidelity. Bayesian optimization, an efficient optimization algorithm, was employed to find the optimal printing parameters while minimizing the number of experiments required. The study considered various bioink concentrations and printer settings as input parameters for the optimization process. The “black-box” model generated recommendations for the experimenter based on visual

assessments of filament morphology and pore architecture in the 3D scaffolds. Optimization continued until an optimal total score was achieved, streamlining the traditionally tedious and time-consuming trial-and-error approach. This research highlights the effectiveness of AI in enhancing the extrusion printability of GelMA and GelMA/HAMA bio-inks. Bonatti, Chua, and De Maria [17] proposed an AI-based quality control loop that automatically optimizes printing parameters for specific materials and printing setups while providing real-time monitoring with rapid response times. They generated an extensive dataset that incorporated videos of bioprinting processes, including parameters such as layer height, extrusion material, infill density, and extrusion system. Pluronic F-127 bioink was used as the primary material, and other materials were simulated by adding color to the Pluronic solution. In order to facilitate quick feedback during bioprinting, they trained a convolutional neural network architecture on the dataset to create a robust model that enables rapid and accurate classification of video frames. The AI model demonstrated excellent classification performance and stability, making it a viable candidate for feedback loop integration. Furthermore, the AI system's rapid response allowed it to monitor successive prints and adjust certain parameters incrementally to resolve potential issues, like varying material properties over time. With this AI-based quality control and optimization approach, bioprinting can be implemented more efficiently, with reduced resource consumption, and enhanced quality assurance.

The adoption of artificial intelligence (AI) in bioprinting has also been used to address the challenge of understanding and optimizing hydrogel ink formulations for 3D printing. Hydrogel-based inks, often incorporating rheology additives, have gained popularity for enabling the 3D printing of biologically relevant materials that were previously non-printable. However, the diversity of these formulations has made it difficult to establish a generalized understanding of printability. Nadernezhad and Groll [18] employed an interpretable machine-learning approach to shed light on the printability process, focusing on bulk rheological indices. This approach was objective and avoided bias toward specific formulation components or rheology additives. Drawing from a vast database of rheological data and printability scores for 180 unique formulations, the study identified 13 critical rheological measures that describe the printability of hydrogel formulations. It was then demonstrated with advanced statistical methods that the collaborative nature of these rheological measures provides a qualitative and physically interpretable guideline for designing new printable materials, even though establishing universal global criteria for predicting printability might be challenging. Their study reveals how AI can offer valuable insights into developing novel, printable materials by deciphering the complex relationship between rheology and printability in hydrogel-based bioprinting. Another study by Huang, Ng, and Yeong [15] examines how AI can be integrated into inkjet-based bioprinting processes to predict and control the number of printed cells within ejected droplets. Two key applications were addressed: firstly, the detection of cell presence or absence in individual droplets, and secondly, the prediction of the total number of cells in multiple droplets. The study employed five machine learning algorithms to evaluate the performance of each model. The first method proved effective for droplets with low cell occupancy but less accurate for those with high cell occupancy. The second method significantly improved cell count prediction accuracy by analyzing the cell count in multiple droplets rather than individual ones, reducing the error in cell count prediction. In addition, the study showed that bio-ink without cells should not be included as input for machine learning models, as it negatively affects model accuracy and overall performance. Overall, this research demonstrated the ability of AI to monitor and control localized cell concentrations within bioprinted droplets, paving the way for precise and dynamic cell placement in bioprinted structures.

### 1.4. The smart bioprinting ecosystem

Presently, Industry 4.0 is revolutionizing advanced manufacturing [16–18] including the biotech/biomanufacturing industry [19]. Another aspect to consider with this is big data. Data is currently the new 'gold' – it is the foundation and engine of every decision and the knowledge derived from data has helped transform the lives of people around the world. As bioprinting evolves, and with the emergence of the bioprinting ecosystem, copious data will be generated from the bio manufacturing process. These may include sensor data, patient records, scaffold designs, medical images, biomaterials, input, and output process parameters [5,14,20–22]. This data will be collected, stored, and processed via the use of cloud computing services. The data will ultimately be employed in developing (AI/ML) models for automation and real-time monitoring of the bioprinting processes [5]. Real time monitoring will also entail the use of NextGen networks such as 5G. According to Sanicola et al. [5], in order to achieve the full potential of a smart bioprinting ecosystem, a cyber-physical system (CPS) architecture that integrates the physical laboratory components (e.g. bioprinters, sensors, computers, and interconnecting devices) with the software components (e.g. machine learning algorithms and data) should be established. The smart bioprinting ecosystem with its multilayered architecture is shown in Fig. 1.

Despite the advanced nature of the smart bioprinting ecosystem, a crucial challenge that must be overcome is security. "The medical industry is ranked among the top 10 most-regulated industries because of its high volume of data and rapidly shifting requirements. Additionally, medical manufacturing is a $156B market and is one of the top five most-targeted industries for cyber-attacks [23]." With the growth of industrialization in the healthcare and medical industry, the potential of attacks on bioprinting infrastructure to inflict damage is a foremost concern. Consider, for example, a case whereby an attacker injects spurious data into software (e.g., ANNs) used in monitoring the printing process or another case in which medical images used in the printing process are manipulated which in turn leads to printing of suboptimal or non-functional bioprinter parts [24]. Therefore, it is important to safeguard smart bioprinting systems against such adversarial cyber-attacks. The research on cybersecurity for a smart bioprinting ecosystem is in its early stages, therefore the primary objective of this paper is to provide a broad and encompassing view of cybersecurity research in the smart bioprinting ecosystem. As illustrated in Fig. 2, the key contributions of this paper are: 1) it extensively reviews and analyzes potential cyber security threats, vulnerabilities, and attacks based on the four facets of the smart bioprinting ecosystem: (AI/ML, Cloud Computing, NextGen Networks and Blockchain technology). 2) it presents privacy preservation solutions in the smart bioprinting ecosystem. 3) it provides a purview of the open research challenges in a smart bioprinting ecosystem. The remainder of the paper is as follows: Section 2 and 3, discusses different internal and external AI/ML threats, respectively. Sections 4, 5, and 6 examine attacks, threats, and vulnerabilities in Cloud Computing, NextGen Network, and Blockchain layers, respectively. Section 7 expounds on privacy preservation solutions. Section 8 highlights Compliance, Regulations, and Standards. Section 9 features open research challenges and potential techniques that can be applied to resolving these challenges. Finally, Section 10 concludes this research paper.

## 2. Internal AL/ML threats

AI algorithms rely on multiple datasets to produce a model with a given set of outputs. In light of this, pertinent safety concerns exist within the domain of AI. These security issues are reviewed in this section. Also, (see Table 1) for a summary of AI/ML threats in the smart bioprinting ecosystem.

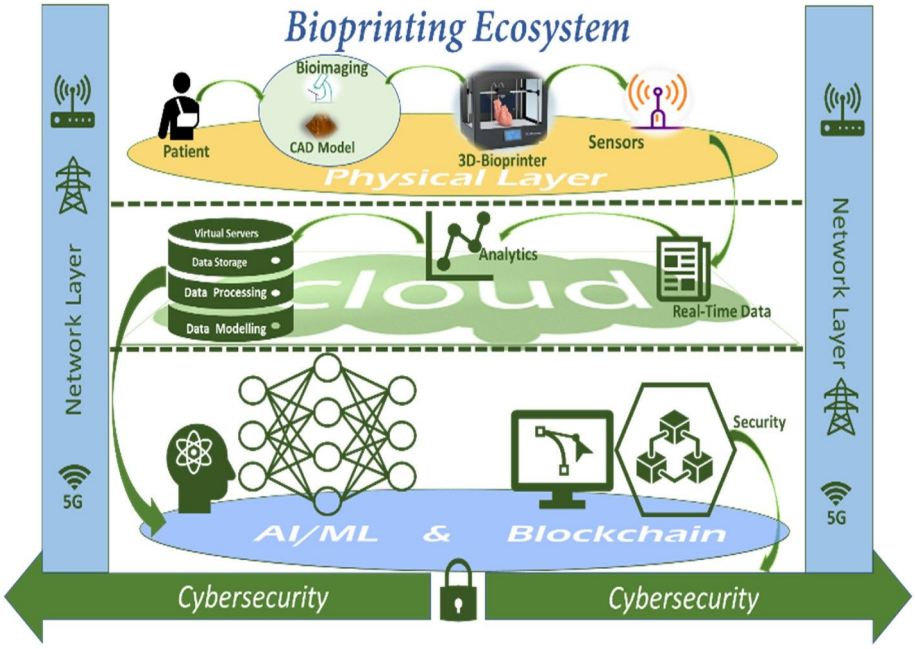



Fig. 1. Multilayered bioprinting ecosystem.

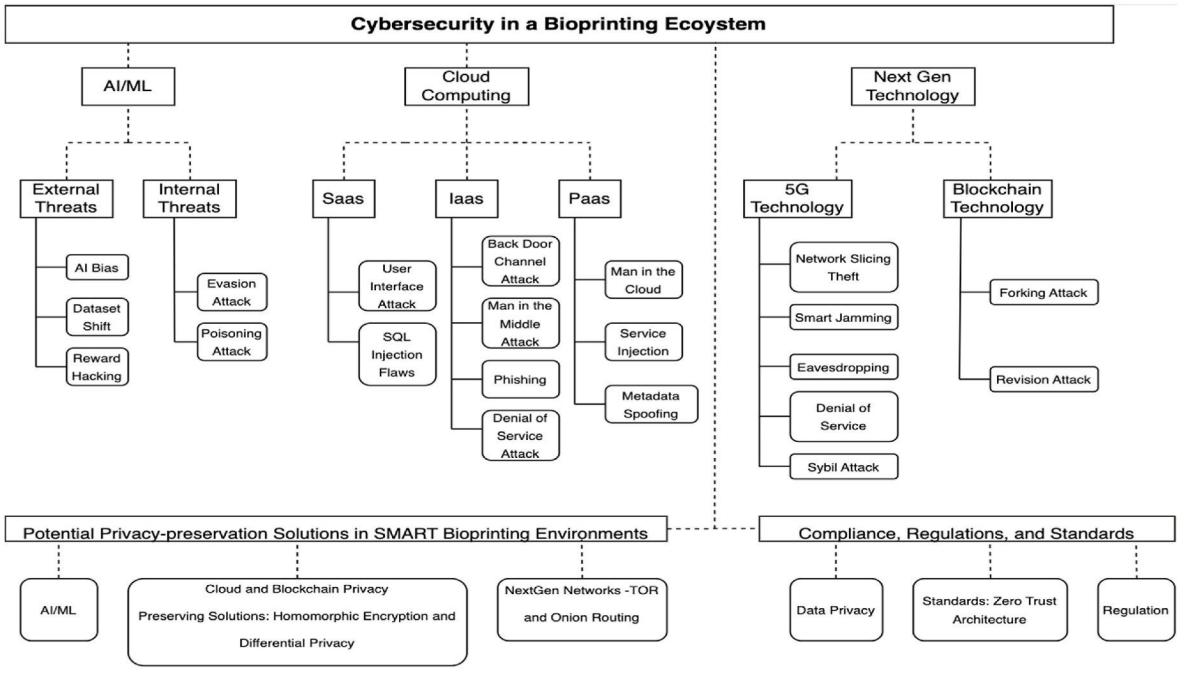



Fig. 2. A taxonomy of cybersecurity in a bioprinting ecosystem.

## 2.1. AI bias

Algorithm bias arises from AI algorithms that produce outcomes with anomalies due to prejudices present in the training data or prejudiced assumptions held by the model's human designer [25]. According to Refs. [26,27], AI bias mainly originates from insufficient training data, the algorithm itself, and the designer (cognitive bias). Cognitive bias stems from a systematic and unconscious error in thinking, which affects an individual's judgment, information interpretation, and decision making. Cognitive bias may inadvertently be introduced in the AI algorithm by the model's human designer or via a poorly curated dataset that contains such biases. The second reason for bias is inherent in the algorithm, specifically, the bias introduced by the algorithm itself. This could be a consequence of the algorithms' "design choices, such as the use of certain optimization functions, regularizations, choices in applying regression models on the data as a whole or considering sub-groups, and the general use of statistically biased estimators in algorithms" [27]. The third reason for AI bias occurs is because of insufficient training data. Training data may not be representative of the true population and thus may include bias.

### 2.1.1. AI bias in bioprinting

AI bias can seep into the bioprinting process if the training dataset contains biased or incorrectly labeled attributes. For example, the

Table 1
Summary of AI/ML threats in bioprinting.

| Threats | | Effects | Countermeasure |
|---|---|---|---|
| Internal Threats. | AI Bias [25–33] | Poses threats such as false positive rates, inconsistencies or high misclassification rate. For instance, a tissue construct which possesses defects may be classified as defect-free resulting in a detrimental effect when the tissue is transplanted into a human subject. | Label Bias Correction, False data injection, Dataset Evaluation |
| | Dataset Shift [34–39] | Poor bioprinting model performance when the AI algorithm/model processes data retrieved from unseen distributions, Reduces the robustness of the bioprinting AI model. | Importance Weighting, Uncertainty Estimation, Generalizing to Unseen Domains via Adversarial Data Augmentation |
| | Reward Hacking [45–49] | Gaming of the bioprinting model's objective function. The agent can game the system by only detecting/recognizing certain types of defects and ignoring the rest in order to accumulate a high reward output. | Shielding, Online User Feedback |
| External Threats | Black & White Box Attacks [47–56] | It can result in deletion of certain feature types such as blood vessels from CT scan images which can be critical to survival of the entire tissue construct. | Black Box: Training Model with private datasets and high input dimensionality, Utilization of Self-developed deep learning models.<br>White Box: Adversarial Training, Randomized Smoothing. |
| | Evasion Attacks [57–60] | High image misclassification rate which can affect the viability and health of the cells within the printed tissue construct, potentially leading to issues post-implantation. | Adversarial Feature Selection, Region Based Classification. |
| | Poisoning [61–67] | Increases bioprinting model's performance error. | Label Flipping correction, Forensic traceback, Reject on Negative Impact (RONI). |

objective of the bioprinting digital twin (a replica of the bioprinting system which comprises two elements: a physical and virtual segment [28,29]) is to classify and predict defective tissue constructs and to optimize input process parameters such as print temperature, feed rate, printing distance, extrusion pressure, and printing speed. Fig. 3 illustrates a digital twin system. Erroneous labels or instances will result in an incorrect model output. Thus, a tissue construct that possesses defects may be classified as defect-free, resulting in a detrimental effect when the tissue is transplanted into a human subject. Another scenario in which AI bias may be introduced in a bioprinting dataset is as follows: a bioprinting ecosystem is developed to assist with creating new skin for burn victims. If the training set containing information about a patient's wound is only fed with information not representative of a population, or for example, data from darker skinned patients is underrepresented. The AI algorithm will be biased towards lighter-skinned patients and will be unable to print new skin tissue that matches a dark-skinned patient's skin tone.

One way to adjust for cognitive bias is to apply the label bias correction method in Ref. [30]. This method assumes that a biased process has altered an unbiased and unspecified label function to create the labels in the training data. Thus, it corrects for bias by altering the sample point distribution through re-weighting adjustments. This method produced an unbiased classifier irrespective of having biased labels as input. Another countermeasure for AI Bias is false data rejection or correction via the introduction of false training data into the algorithm. Their methodology entailed the generation of false training data elicited from the rate of contrasting treatment. This was defined as the difference in the misclassification rate between different groups – the higher the misclassification rate, the more false data generated for that group. The false data aided the improvement of the model's accuracy and thus proved its effectiveness in combating the problem of biased training data due to discrimination. Finally, the training dataset should be thoroughly examined to ascertain if it is representative and substantial enough to inhibit common biases such as sampling bias. For example, subpopulation analysis may be conducted, which encompasses calculating model metrics for particular groups in the dataset [32]. This ensures model performance remains the same within subpopulations. The National Institute of Standards and Technology (NIST) has provided a standard for identifying and managing bias in AI [33].

### 3.2. Dataset shift

A dataset or distributional shift develops when there is a mismatch

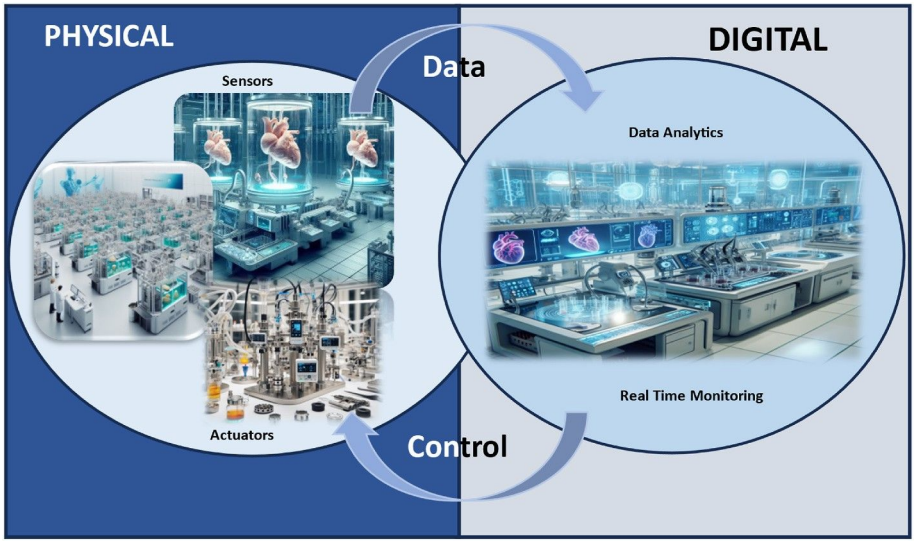



Fig. 3. Bioprinting digital twin system.

between the joint distribution of inputs and outputs between training and test stages [34]. It occurs primarily within the machine learning domains of supervised learning. According to Ref. [35], other reasons behind dataset shift vary from the bias present in experimental design to the irreproducibility of the testing conditions at training time. It also stems from the fact that the data fed into a machine-learning model is mainly characterized using samples from a minimal number of distributions. The shift can also occur when input data is defined by changing demographics [36]. Therefore, the risk of the model performing poorly when it processes data retrieved from unseen distributions increases. Dataset shift is a common problem in AI or machine learning models [35]. The machine learning model's susceptibility to a dataset distributional shift impacts its robustness and may result in less-than-ideal outcomes or situations. It can also produce methodical errors that cannot be corrected by obtaining larger datasets and necessitates specialized methodological care. Krueger and Moreno-Torres [37,38] mention two types of distributional shift in their papers: Covariate and Concept shift. A covariate shift is a change in the input variables (x). In other words, a change in the distribution of inputs over time, while the conditional probability P(y|x) remains unchanged. In contrast, a Concept shift is a change in the relationship between the input and class variables. Specifically, a change in the conditional probability P(y|x). Two examples of dataset shift are discussed in the following sections.

#### 2.2.1. Dataset shift in bioprinting

Dataset shift may be introduced in a bioprinting dataset. For instance, assuming the use case of the bioprinting AI model is to provide a real-time defect detection and monitoring system using historical data from the previous five years. The model in question may have been built using bio-ink materials such as Alginate or Pluronic hydrogels. Supposing the same model is used for defect detection in a situation whereby there has been a change in material composition applied, the model may give a poor performance due to this difference. In medical diagnostics, consider the following real-life example: the case of an ML classifier algorithm built to detect a disease that mostly affected older men. The company in charge of building the ML model was tasked with developing a blood test to be used in curing the disease. Blood test sample data were collected from sick patients within the system and the samples of young healthy men were gathered from students on a university campus. The data collected was used to train the algorithm. It was easy for the ML algorithm to differentiate between healthy and sick people with near-perfect accuracy. However, this would be implausible with real patients because the test subjects differ in age, hormone levels, physical activity, diet, alcohol consumption, and many more factors that were unrelated to the disease. Therefore, a covariate shift would occur because of the sampling procedure.

#### 2.2.2. Dataset shift mitigation

Importance weighting is a technique that has been applied in mitigating dataset shift. It entails reweighting observations according to their "importance weights,"— which is defined as the ratio of their likelihood in target data over input data [34]. Specifically, observations or labels more likely to be present in the target than input data are given higher weights. Dockes, Varoquaux, and Poline [34] refer to another related approach in their work known as "importance sampling"—resampling the training data according to the importance weights. Another technique involves creating models that perform well on unseen data distributions via adversarial data augmentation. Volpi and Murino [39] offer a worst-case formulation for data distributions close to or similar to the work input variables. They use training data from a single input distribution to run an iterative process that amplifies the dataset with examples from a fictitious target domain that is "hard" under the current model. Their iterative procedure is an adaptive data augmentation method wherein adversarial examples are introduced at each iteration.

### 2.3. Reward hacking

Generally, reinforcement learning (RL) uses conventional rewards or objective functions to represent the designer's informal intent. Every so often, the application of these objectives is completed such that the solutions achieved are acceptable in some literal sense but do not attain the designer's objective [40]. In more specific terms, reward hacking occurs in the RL domain, wherein an intelligent agent attempts to manipulate its reward function and locate a strategy that completes a task with very high returns but does so without achieving the designer's intended goal [41].

#### 2.3.1. Reward hacking in bioprinting

The reward hacking problem can be extended to the area of bioprinting, especially with the application of AI models such as reinforcement learning. Bioprinting process parameters include print temperature, feed rate, printing distance, extrusion pressure, and printing speed. These process parameters, along with data extracted from cameras, thermal, and acoustic sensors, can be used to build a digital twin of the bioprinting process. Consider the following hypothetical case whereby the objective of a bioprinting digital twin agent is to create a tissue construct without defects in any layer, i.e., to attain a high-quality print that approximates the intended design and guarantees robust functionality. The agent learns to identify defects or other items of interest from structured data. If the agent prints a defect-free layer, a reward is granted, and if any defect is present in a particular layer, a penalty is applied. Given that there are several types of defects (filament collapse, broken lines, etc.) that may occur during the printing process, the agent can game the system by only detecting/recognizing certain types of defects and ignoring the rest in order to accumulate a high reward output. A mitigation strategy in bioprinting would be to ensure that all process parameters and their expected outcomes are measured and, thus, all possible validation measures applied to construct a bio scaffold structure.

#### 2.3.2. Reward hacking mitigation

Strategies that have been applied in mitigating the reward hacking problem include online user feedback and shielding. In the former strategy, a user (human) is introduced in the training loop to provide online feedback to the agent [42,43]. The user gives uninterrupted feedback to the system in order to update the reward function. To be more specific, each time the agent discovers a strategy with a high reward but negative impact or low user function, the user provides feedback to discourage the agent from its current behavior. Shielding involves the application of a shield to RL such that it ensures the minimum interference and correctness of the system [44]. In other words, the shield evaluates the actions of the learning agent and provides correction only in a case where the learning agent's action is deemed unsafe. Alshiekh et al. [44] applied shielded RL in four main areas: (1) a robot in a grid world, (2) a self-driving car scenario, (3) a water tank scenario, and (4) a Pacman game example. For instance, using a self-driving car scenario, the aim is for the agent to discover how to drive around a block in a clockwise direction in an environment with the size of 480 × 480 pixels. The safety specification of this self-driving car system is to prevent wall collisions. The car was equipped with 8, uniformly attached sensors such that a trigger warning was activated each time the agent was less than 60 pixels away from a wall. A positive reward is assigned for each correct step in a clockwise direction, and a penalty is exacted for each step in a counterclockwise direction. If a wall collision occurs, a penalty is given, and a system restart occurs. The result demonstrated that although the accrued rewards of the unshielded RL increased over time, wall collisions still occurred. The shielded version of the RL agent exhibited rapid learning and experienced no collisions.

## 3. External AL/ML threats

The spotlight is currently on adopting artificial intelligence (AI) and machine learning (ML) models in various application areas. These Machine learning (ML) models are susceptible to adversarial attacks. Several studies have shown that these AI models can be altered at random with subtle and unnoticeable changes to their inputs. These attack types are mainly of two classes: White and Black Box attacks [45, 46].

### 3.1. Black box attacks

A black box attack assumes the attacker has no knowledge of the AI model's network or architecture. In some cases, it only permits querying the network output [47]. For instance, the black box attack in Ref. [48] "has no knowledge of the architectural choices made to design the deep neural network (DNN) which includes the number, type, and size of layers, nor of the training data used to learn the DNN's parameters". Fig. 4 represents a Visual illustration of black-box untargeted attacks. The columns from left to right are original images with correct labels, additive adversarial noises from our attack (gray color means no modification) and crafted adversarial images with misclassified labels. Image courtesy of Chen et al. [49].

#### 3.1.1. Black box attacks in bioprinting

This is the most prominent example of black box attacks. In Ref. [50], the black-box attack assumes the adversary is able to gain access to their image classifier. The attack is a straightforward but very efficient strategy that manipulates the continuous-value confidence score predictions of the classifier. The attack process is based on the premise that "natural images tend to be close to decision boundaries learned by machine learning classifiers". Therefore, a small decision boundary translates to a small and compact search space, and this limits the direction required for perturbation. A random direction can be selected from a pre-specified set of orthogonal search directions. The confidence scores are evaluated against this set of directions to verify their position with respect to the decision boundary. Next, the image is perturbed via addition and subtraction of the vector from the image. The process is repeated such that each update causes the image to deviate from the original image and in the direction of the decision boundary.

Consider a black box attack on the bioprinting AI algorithm that is query-based, and one in which the attacker has no knowledge of its internal structure. The black-box attack can consist of modifying the class of foreground pixels of the images retrieved from the bioprinting process such that there is no effect on the background. Therefore, even though the modification is subtle, it is disruptive enough to trigger the AI model into misclassifying images. An example of this attack type is demonstrated in Ref. [51]. In another bioprinting example, typically MRI or CT scan images are used to build a 3D model of the intended biostructure to be printed (e.g., skin tissue or ear cartilage, etc.). These images are then translated to a 3D modeling software to build intricate features such as the extracellular matrix, vasculature (blood vessels), etc. layer-by-layer using the bioprinter. A black box attack on these image stacks can result in the deletion of certain feature types such as blood vessels which can be critical to the survival of the entire tissue construct. Black box attacks may be hard to discern as the manipulation of certain printed layers may not be identified after the completion of the 3D-printed tissue construct. This type of attack can be debilitating for the patient after implantation due to the lack of functionality of the tissue construct.

#### 3.1.2. Countermeasures/mitigation

Utilization of self-developed deep learning models is one way of mitigating black box attacks. Avoiding the use of open-source models as suggested in Ref. [52] can diminish the likelihood of attacks. This is because, for a self-developed deep learning model, it is difficult to train qualified student models to imitate the teacher model according to the manner in which the black box attack in their study was performed. Therefore, the absence of a qualified student reduces the attack's success rate. A second option that may be considered in mitigating black box attacks is to train the model with private datasets and high input dimensionality. The AI model should be trained using a private rather than a public dataset in order to decrease the chances of an attack. If the AI model within the app is trained on a public dataset, the attacker may discover the same dataset without difficulty. The cost of an attack may be increased by training models with higher input dimensionality or modeling complexity. In Ref. [48], this suggestion was performed, and the results showed that there was a growth in the number of queries needed to train the local substitute model used in their attack strategy.

### 3.2. White box attacks

On the other hand, in a white box attack, the attacker may possess various levels of knowledge about the target model. Knowledge may include the model's parameters, defense mechanisms, gradients, and loss functions. White box attacks differ across models and the application domain. According to Ref. [50], their study poses the argument that in various real-world settings, white-box assumptions are improbable. Their study presented an example whereby the model could be visible to the public as an API and as such, could only permit queries on inputs.

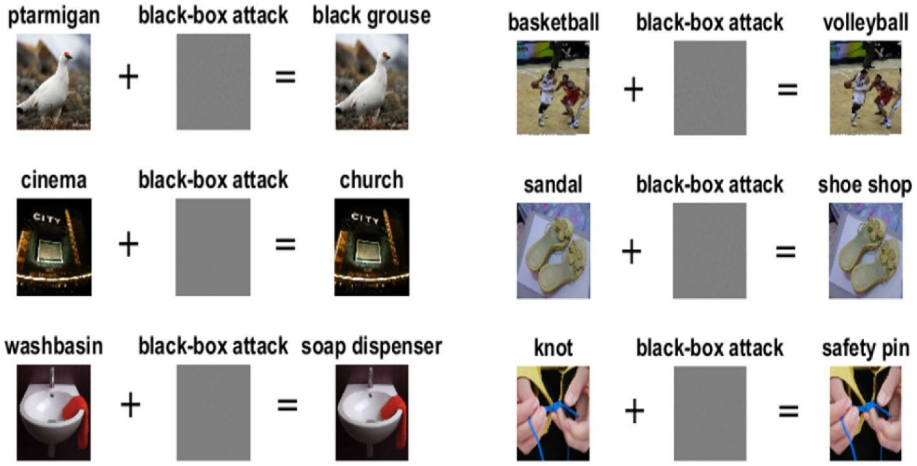



Fig. 4. Visual illustration of black-box untargeted attacks. Source [49].

#### 3.2.1. White box attacks in bioprinting

Assuming a white box attack threat in which the attacker has some knowledge about the AI model such as its input parameters and gradient function, the attacker can manipulate images retrieved from the bioprinting process and cause the AI classifier to classify images that are otherwise free from defects to be classified as defects. This can lead to enormous waste and a colossal increase in process costs. Alternatively, images that are without defects can be classified as defect-free thus subverting the end-use utility of the tissue construct. In bioprinting, maintaining the viability and health of the cells within the printed tissue construct is paramount. Structural health monitoring can be used to evaluate the viability and metabolic activity of the cells during and after printing. It can also be used to uncover any complications that may compromise cell health and provide real-time feedback to the bioprinter, allowing for adaptive printing strategies. For instance, if a structural weakness or cell viability issue is detected during printing, the system can vary parameters such as printing speed, temperature, or material composition to address the problem. In their study, Champneys et al. demonstrate white-box attacks on a data-driven structural health monitoring (SHM) model [53]. The attack consists of two phases: the listening (first) phase and the training (second) phase. In the listening phase, the adversarial transformation network is trained to replicate the inputs, thus generating an inner core model which is then optimized to produce adversarial samples. In the second phase, the network adjusts its internal parameters – weights and biases – so that it maps true inputs to adversarial examples. Their attack success rate was measured by taking the test set of adversarial examples not used during adversarial training and passing them through the perturbing network for classification. The confusion matrix results showed a 99.58 % false-negative classification rate and a 100 % false-positive classification rate.

#### 3.2.2. White box attack mitigation

Adversarial Training and Randomized Discretization is one of the tactics used for mitigating box attacks. It involves constant training of the AI model using adversarial examples. It is one of the few strong defenses against white box attacks. Adversarial-trained AI models have the best low attack success rate when trained with adversarial examples. Specifically, according to Lee [54], attaining a "high accuracy on adversarial examples, not only on clean input samples, has become an important factor in designing machine learning systems." However, adversarial training for white box attacks has mostly been successful in defending against adversarial attacks on small images [55]. For larger images, Zhang and Liang developed a randomized discretization strategy that injects Gaussian noise into individual pixels and substitutes each pixel with the nearest cluster center. Next, it loads the altered image into any pre-trained classifier. Another tactic for mitigating white box attacks is randomized smoothing. Randomized smoothing injects large-scale Gaussian noise into each pixel thereby preventing the likelihood of any small perturbation altering the classifier output. Noise should be calibrated to maintain both accuracy and robustness against adversarial attacks [56]. In other words, the noise should be large enough to preserve robustness and small enough to preserve accuracy. This is because of a decline in accuracy due to an increase in noise intensity.

### 3.3. Evasion attacks

AI systems can be externally compromised through sophisticated malware attacks such as ransomware and botnets. The delivery of the commands, payloads, and other components of these types of attacks must be performed in a clandestine, stealthy, and evasive manner in order to avoid the malware being detected. These give rise to their name–evasion attacks. Evasion attacks are the most prevalent kind of attacks often deployed against AI systems [57]. Evasion attacks involve controlling input data such that it fools a trained classifier at test time. These include feeding the AI algorithm an adversarial example for the manipulation of images to distort object recognition or the manipulation of malware code to have the corresponding sample misclassified as legitimate" [58]. Unlike their counterpart – poisoning attacks, evasion attacks have no influence on training data.

#### 3.3.1. Evasion attacks in bioprinting

Using the same digital twin example from before, there are sensors and cameras mounted on the bioprinting system. Images captured from a mounted camera in the bioprinter are fed into an AI model for classification purposes. These images can be altered through the injection of tiny and unnoticeable perturbations. These adversarial samples can then fool the AI classifier such that the infected image is classified as a genuine image. This can result in the creation of subpar or sub-quality constructs by the bioprinter. Evasion attacks could also affect the viability and health of the cells within the printed tissue construct, potentially leading to issues post-implantation.

#### 3.3.2. Evasion attack mitigation

Zhang et al. [59], proposed an adversarial feature selection method that enhances the generalization capability of a wrapped classifier, and also, provides defense against evasion attacks at test time. The fundamental idea is to select a feature subset that maximizes the generalization capability of the classifier. This mitigation method was applied to the detection of malware in PDF files and Spam Filters and its performance surpassed that of traditional approaches with regard to classifier security. Another mitigation for evasion attacks involves the use of region-based classification. This procedure works based on the premise that adversarial examples are close to the classification boundary." In their study, Cao and Gong [60] develop new deep neural networks that could vigorously withstand state-of-the-art evasion attacks using region-based classification.

### 3.4. Training/poisoning attacks

Poisoning attacks are an external security threat which affects Artificial Intelligence systems. A poisoning attack is one in which a malevolent external agent attempts to manipulate training data or network weights such that it gains influence over the system [61]. Thus, it is denoted as a training-only attack. AI models rely on training data to make accurate predictions, and data poisoning renders these predictions inaccurate. A recent study [62] discovered that 28 organizations identified data poisoning as the foremost threat vector to the security of their AI systems. Therefore, this type of attack poses a serious threat to AI systems, most especially deep learning models – these models employ big training datasets that are scoured from the internet. However, poisoning attacks are not only endemic to neural or deep learning networks, but they can also be observed in regular traditional models such as Naïve bayes [63]. Case in point, a study performed by Biggio, Nelson and Laskov [64] demonstrated that support vector machines (SVM) are susceptible to poisoning attacks. These attacks increased the SVM's performance error. In addition, Nelson et al. [65], revealed that spam filtering algorithms which utilize Naïve Bayes classifiers are vulnerable to poisoning attacks.

#### 3.4.1. Training/poisoning attacks in bioprinting

Poisoning attacks can target the training data extracted from a 3D bioprinter. The infected dataset can be used to fabricate defective or dangerous tissue constructs. This malicious data could also be used to change the properties of the tissue construct, making it unsafe or ineffective. For example, the attacker might introduce subtly altered bioprinting parameters or inject erroneous material properties or environmental conditions into the training dataset, creating inaccurate models that produce suboptimal bioprinted constructs with compromised structural integrity or reduced cellular viability. These attacks could potentially undermine the reliability and effectiveness of a machine learning-driven bioprinting ecosystem.

3.4.2. Training/poisoning attack mitigation

Label-flipping correction is a method used to assuage the effect of label-flippin attacksPaudice et al., developed an algorithm that employed K-Nearest Neighbors (KNN) to relabel points suspected to be malevolent [66]. The objective of the mitigating algorithm was to implement label consistency between instances that were similar, most especially in regions that were distant from the decision boundary. Therefore, k-NN allocated the label to each instance in the training set.

A second method for mitigating poison attacks on deep neural networks was implemented by Shan et al. [67]. The tool developed in their work utilizes an iterative clustering and trimming solution that prunes benign training samples, such that the remnants are the set of poisoned data culpable for the attack. Their algorithm works as follows: in each step, training samples are grouped into clusters based on their influence and effect on model parameters. Next, it detects benign clusters by applying an efficient data unlearning algorithm (a proposed binary measure of event responsibility). The identified benign cluster is denoted as such and excluded from the next clustering operation. Since benign clusters are trimmed, the algorithm "converges on a minimal set of training samples responsible for inducing the observed misclassification behavior."

## 4. Cloud computing

Cloud computing is a new technology that is currently gaining traction as a model for delivering virtual and internet-based computing services. Cloud computing offers a robust and efficient distributed computing model that reduces infrastructure costs and increases an organization's resources by shifting processes performed on an organization's servers to cloud servers. Specifically, it dispenses with the need for training new employees or creating new software packages. Furthermore, cloud computing has been acknowledged as a notable means for offering flexibility, scalability, reliability, sustainability, and affordability of high-quality computing services [68]. A wide range of cloud computing services are currently available today and these can be classified into three major service categories (see Fig. 5) [69]: (1) Infrastructure as a Service (IaaS) – refers to on-demand computational resources in a virtual environment that provides remote services for clients. These include networking, data storage, servers, etc. [68]; (2) Platform as a Service (PaaS) – According to Ref. [70], PaaS provides clients with a complete cloud infrastructure that includes hardware, software, and infrastructure for "developing, running, and managing applications without the cost, complexity, and inflexibility that often comes with building and maintaining that platform on-premises". (3) Software as a Service (SaaS) – in this model, a client utilizes an application software located in the cloud as if it were installed on a local computer, thus allowing several clients to execute the software concurrently.

According to NIST [71], cloud storage infrastructures/environments can be private, public, community, or hybrid. A public cloud environment is one in which the cloud infrastructure is managed by the cloud provider and exists on the provider's premises. In a private cloud, the infrastructure can be managed by an organization, a third party, or a combination of both, and the cloud infrastructure may be present on or off the premises of the cloud provider. The community cloud infrastructure is designed for exclusive use by a specific community of consumers from organizations that have shared concerns and may be managed by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off-premises. The cloud infrastructure is a combination of "two or more distinctive cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability [71]".

Cloud computing plays a major role in modern technology as its application cuts across a vast range of industries including but not limited to healthcare, manufacturing, finance, automotive and education. In the context of this paper, cloud computing will be discussed with respect to the biomanufacturing industry, specifically, the area of bioprinting. The combination of bioprinting and cloud computing can help accomplish extraordinary outcomes such as facilitating an automated workflow of the bioprinting ecosystem, a reduction in the ecosystem's physical and computational costs, and provision of virtual storage facilities. A decrease in computational cost easily translates to faster turnaround times for the bioprinting process. Navale and Bourne [72] proposed cloud adoption in healthcare systems since it offers reliable and safe on-demand storage in addition to flexibility, rapid availability, scalability, and reliability of services. These same benefits will also be extent in a cloud computing and bioprinting combination paradigm. In addition, cloud services have been orchestrated to mitigate big data problems and improve the prospect of "big data and analytics exchange, reproducibility, and reuse". This will prove advantageous in expanding and improving the field of bioprinting in the near future. Navale and Bourne [72] illustrate past and current use cases of cloud services in biomedical work. Despite all the above-mentioned advantages, the bioprinting cloud environment is vulnerable to various types of attacks.

### 4.1. Software as a service

In recent years, the Software as a Service (SaaS) platform has witnessed rapid and progressive use by organizations. SaaS is the most frequently used cloud infrastructure. It operates in the cloud and dispenses with the need for installing and running applications on an organization's physical server or client PC. SaaS provides robust and strong competition against traditional "on site" platforms or models because it is hosted, controlled and maintained by an external cloud

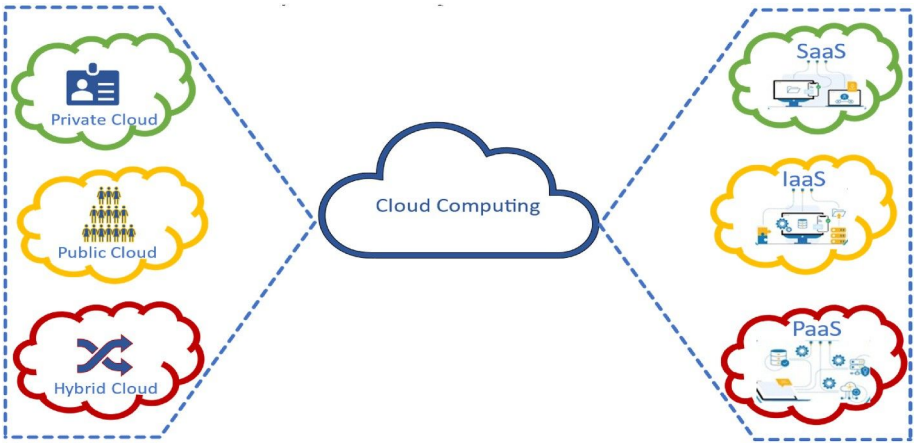



Fig. 5. Cloud storage services (left) and storage infrastructures (right).

provider and is made available to the organization via the Internet as a pay-as-you-go-service. In bioprinting, a SaaS platform also provides a digital avenue for collaboration between users such that these users can individually set up file sharing permissions, design intricate structures, simulate biological processes, and execute 3D printing operations without the need for extensive hardware resources. Data processing in the SaaS cloud platform consists of the following: generation, selection, collection, input, storage, analysis, and output [73].

#### 4.1.1. Security challenges of SaaS in bioprinting

The advancement of SaaS as a sustainable computing platform for bioprinting presents new security concerns. These security threats are

Table 2
Summary of cloud computing threats and vulnerabilities in bioprinting.

| Cloud Computing Services | Threats/Vulnerability | Category/ Type | Attack Mode | Countermeasure |
|---|---|---|---|---|
| Software as a Service | Data Security and Backup [74] | Vulnerability | Data/Security Breach: unauthorized access, exposure, or leakage of sensitive data related to bioprinting processes, bioprinted designs, patient information, or other critical data within the bioprinting ecosystem. | Use of encryption to encryption to protect both data and back up data. Implementation of a concrete data back up plan. |
| | Data Location/ Citizenship [75] | Vulnerability | Data stored and collected from the bioprinting SaaS platform could be subject to legal issues. Inappropriate usage and management of this data poses severe legal consequences. | Provision of a cloud-based resolution which provides regulatory compliance concerning data storage locality |
| | Encryption [76] | Vulnerability | A malicious agent may gain access to decrypted data in the bioprinting database if it uses other methods of cyber-attacks such as email phishing to obtain data such as patient information, proprietary bioprinting CAD designs etc. | Encryption should not be considered a one-shot panacea for data security. Overall system integrity must be protected/preserved in order to ensure total security. |
| | Authentication/ Authorization [77,78] | Vulnerability | These vulnerabilities can be exploited by hackers through the application of brute force attacks, session manipulation, and other similar cyber-attacks to cause data breaches, intellectual property theft, etc. | The least privilege model can be used “with users and CSP (Content Security Policy) administrators only possessing the rights that they require to achieve their tasks. In addition, authentication and authorization be managed externally either by the organization or a third party component |
| | Web Application Security [73–81] | Vulnerability | Application security issues may occur via a design defect within the program or via unreliable configuration of the user interface or web service-based APIs through which the user can access critical assets in the bioprinting ecosystem. | In designing web security tools, common security threats should be considered [73]. These threats/attacks range from database manipulation to large-scale network disruption and include sniffing, |
| | User Interface Attacks [79,82] | Threat | Cross Site Request Forgery is a common web application-level attack that hackers use to circumvent web applications security in order to gain access to the user’s account.<br>In an advanced attack scenario, the attacker may gain full control and disrupt the bioprinting process and other functionalities in the ecoystem. | Clickjacking Defenses, use of CSRF token on webpages. |
| | SQL Injection Flaws [81,83] | Threat | Unauthorized access to the backend database and to the entire bioprinting dataset. Unsanctioned access to the backend database, user lists and the ruin of entire tables are also conceivable consequences of a successful SQL attack | SQL command, Apache rewrite module. |
| Infrastructure as a Service | BackdoorChannel Attacks [87,88] | Threat | An attacker may gain remote unauthorized access to the target bioprinting IaaS server through unsecured points of entry to infect the system with malware. | Use of Multifactor Authentication, Cybersecurity solutions such as Firewalls and Antivirus software. |
| | Man in the Middle [76, 87,89] | Threat | The hacker hijacks a secure encryption connection of data exchange between the user and the bioprinting IaaS server | Traffic encryption [86] and robust isolation between virtual machines. Use of an appropriate secure socket layer (SSL) configuration and the performance of data communication tests between authorized users |
| | Phishing [89] | Threat | The attacker steals or compromises sensitive data within the bioprinting IaaS server system. | Sensitize employees on how to avoid opening spam mails |
| | Denial of Service [87] | Threat | A DoS attack can introduce substantial response delays, extreme losses, and service interruptions, resulting in an immediate effect on the availability of the 3d printing ecosystem. | Use of intrusion detection systems (IDS), Use of Multifactor Authentication. |
| | Man in the Cloud [92] | Threat | The hacker siphons information via access to a synchronization token system employed by cloud applications, thereby illegal access to the cloud system being used to store data from the bioprinting process | Use of encryption to protect cloud data. Use of Multifactor Authentication |
| Platform as a Service | Service Injection [87] | Threat | An adversary can inject a malicious service implementation module or a new virtual machine instance to a PaaS solution for the bioprinting cloud server causing every cloud request from the bioprinting ecosystem to be routed through the falsely injected module or virtual machine. | Application of a service integrity checking module. Implementing strong isolation between VMs. |
| | Metadata Spoofing [87,93] | Threat | An adversary may modify or change the Web Services Description Language (WSDL) to gain access and take advantage of these metadata and use them for malicious purposes such as intellectual property theft, regulatory compliance failures. | Use of encryption to protect cloud data. Use of Multifactor Authentication |

discussed in the next subsections and are summarized in Table 2.

4.1.1.1. Data security and backup. The bioprinting cloud system process will comprise data collection, preprocessing, storage, and analysis. The advent of data processing in SaaS comes with the risk of a data breach, making it a top security concern. In the bioprinting ecosystem, this can be extremely dangerous because patients' data can be stolen thus violating patient privacy and laws such as the United States Health Insurance Portability and Accountability Act (HIPAA laws). Data security in SaaS becomes particularly challenging in a case where it is handled by a third-party SaaS provider. Another vital facet of SaaS security is data backup [74] – the SaaS service provider must ensure that there is a concrete backup plan for data. This will prove critical in improving and accelerating recovery time in the event of a cyber-attack or other similar security breach. The SaaS provider can use robust security tools such as encryption to protect both data and backup data. The SaaS provider may also employ the services of a third party to provide backup solutions.

4.1.1.2. Data location/citizenship. One vital aspect of processing, transmitting, and storing data in the cloud is where this data ends up. Specifically, a widespread compliance issue many organizations need to confront is that of data location. Bioprinting data – such as patient data and design files – that is stored and collected from the bioprinting SaaS platform could be subject to legal issues. Inappropriate usage and management of this data poses severe legal consequences. Therefore, the onus rests on the cloud SaaS provider to offer a cloud-based resolution that provides regulatory compliance concerning data storage locality [75].

4.1.1.3. Encryption. There are three major levels at which data can be encrypted: in transit, at rest, and in use [76]. The data transmitted between remote devices as observed in the cloud environment is encrypted during transit and at rest. Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocol is used for securing data in transit over the web. However, encrypting data in transit does not necessarily provide total protection from cyber-attacks. According to Ref. [76], "encrypting data in transit can be compromised even if it is being performed across both internal and remote networks via the placement of malware on authorized devices which can eavesdrop or sniff data as it traverses the enterprise" [76]. Therefore, encryption should not be considered a one-shot panacea for data security in the bioprinting ecosystem. For instance, a malevolent entity will still be able to gain access to decrypted data in the bioprinting database if it uses other methods of cyber-attacks such as email phishing to obtain valid user credentials.

4.1.1.4. Authentication and authorization. Authentication and authorization are the two most crucial aspects of SaaS application security. The manipulation of authentication and authorization vulnerabilities is a frequent occurrence. These vulnerabilities can be exploited by hackers through the application of brute force attacks, session manipulation, and other similar cyber-attacks. SaaS security best practices establish whether a user ought to be given legitimate access (authentication) supervened by access levels and roles (authorization). Authorization for access to data could be done based on an organization hierarchy access policy that is evaluated periodically. The Federal Office for information security [77] suggests the least privilege model be used "with users and CSP (Content Security Policy) administrators only possessing the rights that they require to achieve their tasks." Another suggestion by Ref. [78] is that authentication and authorization be managed externally either by the organization or a third-party component.

4.1.1.5. Web application security. A "must-have" requirement for a SaaS application is that it has to be employed and controlled over the web. Security gaps in the worldwide landscape of the internet make a bioprinting SaaS application vulnerable to cyber-attacks of different levels of scale and complexity and from different sites or locations around the world. Hence the a need for tools that provide security countermeasures for web applications and services especially those involved in cloud service operations. Application security issues may germinate at various stages of application design, development, implementation, and access to a bioprinting digital twin system. Consequently, it can be affected by a design defect within the program or via unreliable configuration of the user interface or web service-based APIs through which the user can access the application [79]. In designing web security tools, common security threats should be considered [80]. These threats/attacks range from database manipulation to large-scale network disruption and include sniffing, XML spoofing [81], denial of service (Dos), SQL injection, cross-site reference scripting and cross-site request forgery.

4.1.1.6. User interface attacks. Every SaaS application comprises four types of multi-tenanted user interface entities. "They include a) client software organization structure and components, b) user interface forms with styles, c) events, and d) user operation flows [82]." Bioprinting generates complex datasets, including 3D models, patient profiles, and experimental results. Multi-tenancy facilitates controlled data sharing among tenants, enabling enhanced integration and analysis of data for comprehensive insights. Therefore, a bioprinting SaaS application will entail the use of a collection of interfaces and APIs which enables the implementation and execution of several client operations. Clients can relate with the SaaS application via client feedback fields. However, if these feedback fields do not authenticate the client's input or retrieve valid data, they may be manipulated by malevolent entities via injection attacks [79]. For instance, using an approximation of the CSRF example in Ref. [79], suppose there is a situation in which a client or end-user is authenticated to a bioprinting SaaS applications site, a user can inadvertently click on an infected website that is within the grasp of a malevolent entity, the entity can forge malicious requests and implant its attack in an image on the website under its control.

4.1.1.7. SQL injection flaw. Web applications work hand in hand with SaaS cloud service and as a result, most of the security threats faced by web applications can also be encountered in a cloud SaaS platform [81]. As mentioned in the previous section, an SQL injection attack is one such web application threat. It is a type of attack vector that exposes the vulnerability of the SaaS cloud service platform. In this type of attack, a malicious SQL code is used to alter the backend database and gain unauthorized access to the entire bioprinting dataset. Unsanctioned access to the backend database, user lists, and the ruin of entire tables are also conceivable consequences of a successful SQL attack. The Rewrite module of the Apache server may be used as a precaution against SQL injection attacks. Another mitigation technique is that of SQL randomization also known as SQLrand. This technique was devised by Boyd & Keromytis [83] and develops instances of the language that are indecipherable to the attacker. In particular, the technique thwarts queries inserted by an attacker.

### 4.2. Infrastructure as a service (IaaS)

Infrastructure-as-a-Service, generally referred to as "IaaS," is an aspect of cloud computing which refers to the fundamental element of computing that can be rented on a pay-as-you-go basis. It consists of physical and virtual resources that deliver the foundation required to run applications and workloads in the cloud. IaaS components include data storage, network, virtual and physical servers, and other shared resources. IaaS relieves the user of the task of operating and managing the virtual and physical infrastructure, and at the same, offers them control over the operating system, configuration, and software running on the virtual machines in order to create user-controlled applications [84,85]. Unlike PaaS and SaaS, IaaS gives the lowest-level control of resources in the cloud [85]. Cloud computing services like IaaS can have

a gigantic impact on the manufacturing industry which is a part of the proposed concept for the 4th industrial revolution [86], especially in the area of bioprinting which is the focus of this paper. For instance, data processing time is a computational bottleneck for executing image analysis tasks. In addition, the application of deep learning methods on such tasks can lead to drastic improvements in quality assurance for tissue constructs. Implementing deep learning techniques often necessitates the use of multiple GPUs for processing "large batch sizes or reducing batch sizes while training the algorithms" [5]. Cloud computing services such as IaaS offer a novel way of eliminating this problem. However, employing the above-mentioned IaaS components together in a shared and outsourced environment poses various challenges, amongst which security is the most important challenge that can hamper the consolidation of bioprinting with cloud computing platforms. The next section discusses security issues/threats that affect IaaS along with their proposed solutions.

#### 4.2.1. Backdoor channel attacks

This is a passive attack in which a hacker attempts to gain inside information about the IaaS machine, network, or other systems used in processing bioprinting data without detection. A backdoor channel can allow a hacker to gain remote unauthorized access to the target bioprinting IaaS server system through unsecured points of entry and spread malware in the system or make it a zombie for attempting a DoS attack [87]. For instance, research conducted by Eclypsium [88] "revealed firmware vulnerabilities in Supermicro systems that would allow malware to install backdoors and rootkits to steal information". They discovered weaknesses in server update procedures for Bare Metal Cloud services (a cloud service provider) firmware that would enable an attacker to install malicious BMC firmware. They also demonstrated how this type of attack could be used to permanently "brick" a server. Backdoor channel attacks can be mitigated using multifactor authentication, and cybersecurity solutions such as Firewalls and Antivirus software.

#### 4.2.2. Man-in-the middle attack

This type of attack exploits vulnerabilities in the network, web browser, or server OS. It allows the hacker to hijack a secure encrypted connection or data exchange between the user and the bioprinting IaaS server. According to this paper [89], "Man-in-the-middle attack "is the one thing that breaks the security paradigm for encrypted data in transit" [89]. Modi et al. [87] suggest the use of an appropriate secure socket layer (SSL) configuration and the performance of data communication tests between authorized users in order to reduce the occurrence of this type of attack. Another mitigating element is to ensure traffic encryption [76] and robust isolation between virtual machines.

#### 4.2.3. Phishing attack

In a phishing attack, the attacker attempts to steal or compromise sensitive data within the bioprinting IaaS server system. Phishing is often the "tip of the spear" or the first part of an attack to hit a target [88]. In Cloud IaaS systems, it may be possible that a hacker could compromise the bioprinting IaaS cloud system to host a phishing attack site to hijack login credentials and therefore gain access to the accounts and services of other users in the Cloud. To avoid phishing, the organization will need to be able to sensitize employees on how to avoid opening spam emails. The following elements may be used in identifying such emails, "Poor spelling and grammar", suspicious links or attachments, urgent calls to action, unrecognized sender, etc.

#### 4.2.4. Denial of service

This attack focuses on disrupting the operation of a resource such as a website, a server, or an application. An IaaS DoS attack on the bioprinting IaaS system could occur through the compromise of a user's virtual machines, a VM level attack, a Hypervisor level attack, or a Network level attack [87]. Typically, bioprinters are composed of different sub-units to dispense a variety of biomaterials to form an intricate functional tissue structure. Examples of sub-units include an extrusion head, inkjet head, laser scanner, optical microscope, and nebulizer to name a few. A denial-of-service attack on any one or combination of these devices can significantly hamper the fabrication of functional tissue constructs. This is because many biomaterials used in these sub-units have limited shelf-life (varying from minutes to a few hours). A DoS attack will render these materials useless and more importantly fatal to the end-user if degraded biomaterials are encapsulated within the tissue construct. A good mitigation strategy is to establish intrusion detection systems (IDS) and to provide strong authentication (e.g., uses multi-factor authentication (MFA) to authenticate a user's identity) and authorization.

### 4.3. Platform as a service

The Platform as a Service (PaaS) is a development platform that permits users to develop their services and applications in the cloud. It also assists the entire web application lifecycle: design, implantation, testing, validation, deployment, and maintenance [90]. The major difference between PaaS and SaaS is that the latter only accommodates complete cloud applications while PaaS offers a development platform that accommodates both completed and in-progress cloud applications [91]. Google App Engine is an example of a PaaS platform. It allows developers to write and run their applications on data centers managed by Google. It also provides a defined application model and a set of APIs which allows developers the benefit of using bonus services like Mail, Namespaces, Datastore, Memcache, etc. Other examples of PaaS providers are AWS Elastic Beanstalk, Microsoft Azure, Salesforce aPaaS, Red Hat OpenShift PaaS, Mendix aPaaS, IBM cloud platform (a combination of IaaS and PaaS), and Oracle cloud platform. According to Statista, PaaS revenue in the Platform is projected to reach US$79.55bn in 2022 with an annual growth rate (CAGR) of 20.23 % from 2022 to 2026. It is expected that the global market size of PaaS will reach US$166.20bn by 2026. It should be noted that PaaS, SaaS, and IaaS each possess their individual security issues. In PaaS, the applications and services offered by the PaaS platform are shared among multiple customers thus introducing a multitenancy aspect. Consequently, a proper isolation mechanism must ensure that one tenant cannot access components of other tenants. In the context of the bioprinting ecosystem, PaaS can transform how researchers and clinicians handle tissue engineering and medical device creation. PaaS platforms can incorporate design, simulation, and printing processes into a seamless workflow. This integration streamlines the bioprinting pipeline, reducing manual data transfers and potential errors. As sharing mechanisms in the cloud computing platform become more widespread, and despite all the above, security remains a top prevailing concern, especially with the adoption of PaaS and other cloud computing elements in the bioprinting ecosystem. The security threats relating to PaaS are discussed in the next subsections and are summarized in Table 2.

#### 4.3.1. PaaS security challenges

##### 4.3.1.1. Man-in-the-cloud (MiTC).

An adversary can siphon information via access to a synchronization token system employed by cloud applications. The omnipresent nature of the cloud translates to the same token being used to authenticate a user's credentials repeatedly and irrespective of a change in device. MiTC commences when an adversary successfully installs a malicious code on a target's device in the bioprinting ecosystems in order to access a user's synchronization token [92]. Thus, bypassing security measures and granting the adversary illegal access to the cloud system being used to store data from the bioprinting process. To mitigate the probability of MiTC attacks, the use of encryption to protect cloud data should be implemented. Secondly, a multi-factor authentication system for verifying a user's identity in the

bioprinting ecosystem should be adopted.

4.3.1.2. Service injection attack. In a service injection attack, an adversary can inject a malicious service implementation module or a new virtual machine instance into a PaaS solution for the bioprinting cloud server [87]. If the attack is successful, every cloud request from the bioprinting ecosystem will be routed through the falsely injected module or virtual machine. This can lead to data theft or eavesdropping. Injection of malicious commands could also disrupt ongoing bioprinting experiments, potentially damaging valuable biological materials and delaying research progress. To protect the cloud system from this type of attack, Modi et al. [87] recommend the application of a service integrity checking module. In addition, they suggest a "strong isolation between VMs" to prevent the spread of malicious code to neighboring VMs.

4.3.1.3. Metadata spoofing. Every device generates metadata based on a user's request. According to NGINX [93], certain cloud providers offer "a service (in the form of an API) that enables services running in a virtual machine to query "instance metadata", which can include sensitive data such as authentication credentials". An adversary may modify or change the Web Services Description Language (WSDL) to gain access and take advantage of these metadata and use them for malicious purposes. The authors in Ref. [93] discuss how an overly permissive configuration makes it easy for the manipulation of metadata stored on the IP address employed by the above-mentioned cloud service providers. In the bioprinting instance, a temperature sensor will be connected to the internet using a wireless network. This sensor will transmit data to the cloud. An adversary may exploit the metadata generated during this process by accessing the internal IP address illegally. The adversary could also alter metadata to falsely claim authorship of valuable bioprinted designs, leading to intellectual property disputes and potential financial losses. To mitigate a metadata spoofing attack, Modi et al. [87] recommend the implementation of encryption and strong user authorization and authentication in the cloud system.

## 5. Next-generation networks: 5G technology

The last two decades have witnessed the rapid evolution of cellular communication systems. These include 2G, 3G, and 4G communication network systems. The driving factor behind the evolution of these technologies has been the need for low latency and more bandwidth. According to Ref. [94], "The data rate has improved from 64 kbps in 2G to 2 Mbps in 3G and 50–100 Mbps in 4G" [94]. However, users are withdrawing from legacy 2G/3G technologies and moving toward 4G/5G systems. In fact, 5G systems are currently the focal point of the manufacturing, energy, healthcare, and transportation industries, as well as government and academia. This is because 5G technology offers many innovative benefits for different industry network requirements. These benefits include but are not limited to ultra-low latency, reduced cost, energy efficiency and sustainability, high speed, and ultra-reliable communication [95–99]. Additional benefits include the enhancement of mobile network bandwidth, which will eventually lead to an upsurge in the number of IoT devices that can be connected at a given time. It has been envisaged that twenty-seven billion IOT devices are expected to be connected by the year 2025 [100]. A significant proportion of these devices will be connected via 5G technology.

The implementation of a bioprinting ecosystem will consist of physical laboratory components, (such as computers, bioprinters, robots, sensors, and other IoT devices), biomaterials, and software components such as cloud computing software, AI, and optimization algorithms [5,101]. Connectivity is a crucial facilitator of Industry 4.0, and it is a notable aspect of the bioprinting ecosystem to consider, especially with the advent of IOT devices which enable digital systems to record, monitor, and fine-tune each interaction between linked devices. The connectivity needs for the multitude of connected devices in the bioprinting ecosystem will be handled via 5G technology. An example of 5G implementation in healthcare is seen in Yongjian et al. [102]: a Guangdong Provincial People's Hospital applied AI and 5G technology in a live broadcast of a traditional cardiovascular surgery. The experts/consultants who strategized the surgery's plan were in Guangzhou, while those who were in charge of the actual operation were in Gaozhou. The distance between both locations is 1158 miles. Hence, the use of 5G technology as a guide for the operation in real-time 5G technology will facilitate the creation of a digital twin of the bioprinting ecosystem. A digital twin comprises two elements: a physical and a virtual segment [29] as seen in Fig. 2. The physical aspect deals with the collection and storage of data – this data will be stored in the cloud. Data will be retrieved from the bioprinting process via acoustic, infrared, and temperature sensors which are connected to the Bioprinter. The virtual aspect consists of employing the data retrieved in the physical segment to perform real-time simulation and analysis of the bioprinting process. The real-time exchange of information in the bioprinting ecosystem calls for ultra-low latency and highly reliable communication. In a nutshell, NextG wireless networks such as 5G form the building foundation for two-way communication between the digital twin and the physical aspect of the bioprinting ecosystem. However, 5G technology also presents its challenges, security being the foremost [103]. The next section discusses the security threats posed by using 5G technology. A Summary of NextGen Network Threats is also presented in Table 3.

### 5.1. Security threats in 5G technology

#### 5.1.1. Network slicing attack (slice theft)

The core of the 5G network is a paradigm that enables communication resources and attributes to be split into individual slices. Each slice is isolated from one another. If an adversary can gain access to a cloud network function, it could potentially exploit security shortcomings in current 5G industry standards to gain access to both the operator's core network and the network slices of other enterprises. A bioprinting ecosystem consists of several interconnected mechanisms, such as bioprinters, data storage and real-time monitoring components, and potentially even communication networks that facilitate the transfer of data and instructions. Consider a case whereby the bioprinting ecosystem is dependent on a high-speed and low-latency 5G network to transmit complex 3D bioprinting instructions and data. Various stages of this process might involve designing the tissue structure, obtaining the appropriate cells or bioinks, and executing the actual bioprinting. The network slices ensure each stage has the required bandwidth, latency, and quality of service to function optimally. An adversary could use a network slice attack to disrupt the communication between different components in the ecosystem, manipulate bioprinting instructions, or steal sensitive data related to patient-specific tissues being printed. To protect against network slicing attacks, Shi et al. [104] introduced various defense mechanisms such as stopping Q-table updates when an attack is detected, employing randomness in making network slicing decisions, exploiting the feedback process in network slicing in order to distort the attacker's learning process. Their research demonstrates an effective method of defending network slicing by tricking/misdirecting an adversary into making incorrect decisions and thus, reducing the risk of an attack.

#### 5.1.2. Smart jamming

A jamming attack can be defined as a malicious disruption of data communication in the bioprinting ecosystem. The intention of the adversary in this scenario is to cause an interference in the bioprinting ecosystem's network. There are several types of jamming attacks and these have been discussed in detail in Pirayesh & Zeng [105]. For instance, a reactive jamming attack, also referred to as a channel-aware jamming attack entails the adversary transmitting an interfering radio signal when it detects legitimate packets transmitted over the air.

Table 3
Summary of NextGen network threats in bioprinting.

| Technology Type | Threats | Mode of Attack | Countermeasure |
|---|---|---|---|
| 5G Technology | Network Slicing Theft [104] | An adversary can gain access to a cloud network function by exploiting security shortcomings in current 5G industry standards to gain access to network slices dedicated to bioprinting. | Stopping Q-table updates when an attack is detected. Employing randomness in making network slicing decisions. Exploiting the feedback process in network slicing in order to distort the attacker's learning process |
| | Smart Jamming [105,106] | An adversary transmits an interfering radio signal to disrupt or compromise the communication and control systems used in the bioprinting ecosystem. | Observing communication channels for any surplus amount of energy or any unexpected shift in the communication performance over the channel. |
| | Eavesdropping [103,107] | An adversary takes advantage of an unsecured network in the bioprinting ecosystem and intercepts data sent or received over the network | Encryption of signals via wireless connections. |
| | Denial of Service [107], [109] | A hacker manipulates the bioprinting network's service by overloading its capacity or exhausting its resources | Implementation of a dos detection system. |
| Blockchain | Sybil Attack [122, 123] | An adversary can generate multiple fake or malicious identities or nodes within the bioprinting blockchain network to manipulate or disrupt bioprinting related processes and transactions. | Use of validation and chain of trust systems. |
| | Forking Attack [124] | A forking attack may occur when an adversary is unable to modify records on the main trusted chain (MTC) of the bioprinting blockchain network. The adversary thereby launches an alternative or side chain to replace the MTC. | Use of an MTC confirmation mechanism whereby an arbitration mechanism compels branches from a fork to engage in a competition. |
| | Revision Attack [125,126] | A revision attack alters the blockchain's forking rules such that it allows for genuine historical bioprinting-related data or transactions to be replaced by an alternative history, "from the forking point onwards" | Use of digital signatures to verify the authenticity of transactions in the bioprinting blockchain network, and to guarantee that these transactions cannot be modified without detection. |

Jamming attacks can be mitigated by observing communication channels for any surplus amount of energy or any unexpected shift in the communication performance over the channel. According to Arjoune & Farugque [106], one common tactic in jamming detection is setting a threshold detection value by monitoring the channel in the presence and absence of a jamming attack using "performance metrics such as the packet delivery ratio (PDR), packet drop ratio (PDR), bit error rate (BER), and signal-to-noise ratio (SNR)".

### 5.2. Eavesdropping attacks

This is a passive attack in which an adversary takes advantage of an unsecured network and intercepts data sent or received over the network [103]. Eavesdropping may also be referred to as a snooping or sniffing attack [107]. The bioprinting communication network presents a ripe target for this type of attack, given that there would be real-time monitoring of the printing process, in addition to large transmission of data such as build temperature, print speed, federate, flow rate, speed ratio, build chamber temperature and so on. An eavesdropping attack is considered passive because the data or information being transmitted is usually not disturbed or altered; the aim of the adversary is to secretly obtain information. As a result of its passive nature, it is usually difficult to detect. This type of attack can compromise sensitive and confidential infrastructure, especially for defense and national security-related bioprinting ecosystems. Encryption of the signals via a wireless connection is the most common method of mitigation. The use of encryption prevents the eavesdropper from intercepting the received signal. Information picked up from eavesdropping attacks can be used to perform denial of service (DoS) attacks.

#### 5.2.1. Denial of service attacks

This is an active type of attack in which the adversary manipulates the bioprinting network's service by overloading its capacity or exhausting its resources [107] thus, making the network unavailable to users for a period of time. DoS is a severe attack that can partially or devastate a bioprinting ecosystem's network. Such an attack can result in tissue construct printing delays, sub-quality tissue constructs, material wastage, and increased cost. Unlike eavesdropping attacks, in DoS, the adversaries typically do not attempt to steal or modify information. However, DoS is one of the most prominent cyber-attacks because of the cost of inaccessibility of services on the part of casualty networks or systems. The common mitigation method for DoS is detection [108]. For instance, in their paper, Kuadey et al. [109] proposed a deep Secure framework that entails the use of user equipment (UE) devices, an attack detection model, a slice prediction model, an infrastructure provider, and network slices. Their attack detection model forecasts DDoS attacks from the UE network traffic, "while the slice prediction model predicts suitable slices for legitimate UEs".

## 6. BlockChain networks

Blockchain began to gain traction when Satoshi Nakamoto conceptualized [110] the first blockchain in the year 2008. Ever since technology has experienced innovative modifications and improvements. Blockchain technology can be described as a distributed peer-to-peer database distributed network ledger that comprises a chronological sequence of blocks [111,112]. Blockchain technology is considered to be very secure due to its inherent characteristics [113–115] of immutability, decentralization, traceability, reliability, low cost, transparency, transaction automation, and anonymity, in addition to its ability to perform cryptographic transactions. Fig. 6 represents the various characteristics/features of Blockchain technology.

Blockchain can utilize a decentralized consensus protocol and digital signature to validate and authenticate the integrity and accuracy of the transactions performed between all parties in the bioprinting ecosystem's network [116]. This will enhance the security and integrity of critical bioprinting data, such as patient information, tissue specifications, and printing instructions. This can also help assuage issues such as data security [117], counterfeiting [118], and IP theft [119]. Blockchain's smart contract functionality can automate certain aspects of the bioprinting process. For instance, when certain conditions are met (e.g., successful completion of specific printing stages), predefined actions could be triggered automatically, improving efficiency, and reducing the risk of human error.

In terms of counterfeiting prevention, taking additive manufacturing for instance, component designers can adopt blockchain technology to ensure that only authorized users will be able to access design files and submit information. This inhibits access to the design files until they are deleted by AM-designated machines [120]. Presently, most bioprinters do not come equipped with sensors. Specifically, the bioprinter's control mechanism and sensor data retrieval are not explicitly linked [121], therefore, these printers are enhanced using sensors that are not

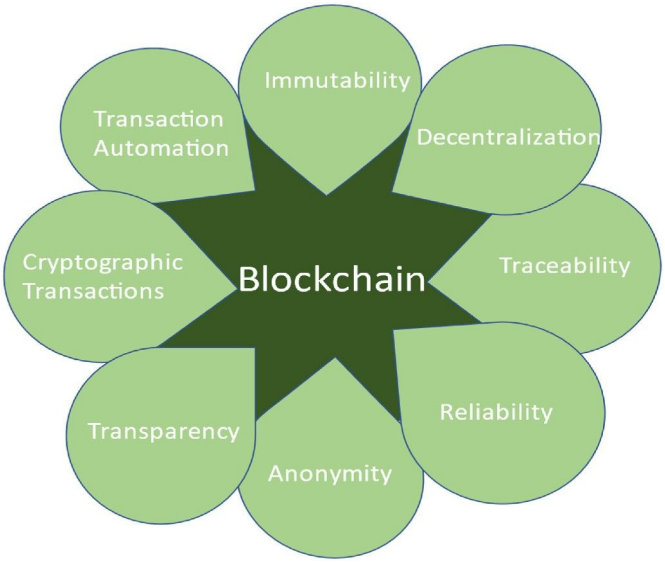



Fig. 6. Features of blockchain technology.

included in the original equipment manufacturer (OEM) catalog. Furthermore, the information extracted from these sensors is distributed to and stored in the cloud network. This information is extracted from the cloud for advanced analytics and real time monitoring of the bioprinting process. Blockchain technology can be used to transact records of sensor data between distinct sections of the bioprinting ecosystem [121]. However, it also suffers from security issues such as those discussed in the next section. A Summary of these threats is given in Table 3.

### 6.1. Security threats in BlockChain technology

#### 6.1.1. Sybil attacks

In a Sybil attack, an adversary can control multiple identities (Sybils) and force negative feedback in order to make a trusted device appear untrustworthy to its peers or an untrustworthy device appear trustworthy" [122]. A Sybil attack in the bioprinting blockchain network can be used to obtain information about the IP addresses of connected users. This poses a risk to the security and anonymity of the networks' users. Sybil attacks can be prevented via the use of validation and chain of trust systems. Otte et al. [123] created a "permission-less tamper-proof data structure for storing transaction records of agents" called TrustChain. TrustChain utilizes a sybil-resistant algorithm called NetFlow to ascertain the credibility and "trustworthiness of agents in an online community." Their model ensures that "free riders" are identified. In other words, agents that retrieve data/information from the online network also contribute back to the network.

#### 6.1.2. Forking attack

A fork in the blockchain is a representation of two or more chain branches generated from a block and this occurs when two or more miners solve the hash function concurrently. In the bioprinting blockchain network, a forking attack may occur when an adversary is unable to modify records on the main trusted chain (MTC) of the network [124]. The adversary thereby launches an alternative or side chain to replace the MTC. This alters the blockchain's authority, making fraudulent records on the sidechain appear legitimate in order to gain access to records in the blockchain. Wang et al., suggest a novel MTC confirmation mechanism whereby an arbitration mechanism compels branches from a fork to engage in a competition [124]. The main chain contends with the sidechain in the arbitration section until it achieves an end threshold. This end threshold is set to guarantee the main chain wins the competition if the fork structure is formed by a forking attack.

#### 6.1.3. Revision attack

Short-lasting forks are often encountered in blockchains; however, they are usually corrected because of the blockchain rule – the chain with the most difficulty wins. This mechanism is effective, under the hypothesis that an adversary can never obtain the extremely high computational power required to forge a different or alternative history [125,126]. If this is the case, an adversary can perform a so-called history revision attack such that the blockchain's forking rules allow the genuine history to be replaced by the alternative history, "from the forking point onwards" [125]. There is yet to be a formal anti-revision attack strategy in the literature. However, a possible mitigation strategy would be the use of digital signatures to verify the authenticity of transactions and guarantee that such transactions cannot be modified without detection. For now, such an attack might be considered improbable due to the enormous computing power needed.

## 7. Potential privacy-preservation solutions in SMART bioprinting environments

### 7.1. Artificial intelligence/machine learning

The collection of personal data from the bioprinting ecosystem will be considerably easier with the use of AI, IoT devices, and Cloud Computing. However, even though AI models improve with the availability of private data, there are also significant consequences associated with this data collection. Specifically, the use of AI further compounds issues by generating data and using it in ways that were previously not possible. For instance, as bioprinting technology develops, bone and tissue information can be collected in order to build a customized biofabricated product for a particular patient/individual. In addition, the bioprinting ecosystem is a cyber-physical system, and as such, one common area to take into consideration is the ''privacy'' and confidentiality of the patient's information [32]. It becomes problematic if an attack occurs and the patient's data is hijacked thereby breaking laws such as the United States Health Insurance Portability and Accountability Act (HIPAA laws). Perceived risks to privacy and security may possibly undermine patient/client confidence necessary for bioprinting to reach its full potential. It is highly crucial to manage such sensitive data in a way that protects privacy. In the medical field, anonymization– processing data in an irreversible way and with the intent of preventing re-identification, and pseudonymization – ('replacement of sensitive entries" with values that do not allow an individual to be directly identified [127], are two distinct techniques that offer regulation compliance, data security and privacy. These two methods are also applicable to the bioprinting stratosphere. A more promising mitigation technique to the AI data privacy attack issue is Federated Learning (FL). FL as proposed by Google researchers [127], is a technique that employs the use of a ML model in a decentralized shared learning setting such that the ML algorithm is executed using local client-side devices and local training datasets. FL dispenses with the need to send data to a centralized server, instead, an "extraction in the form of machine learning models is sent to the server" [128]. Simply put, "FL brings the code to the data, instead of the data to the code, and addresses the fundamental problems of privacy, ownership, and locality of data". A real-life example application of federated learning is a study conducted by Mass General Brigham and NVIDIA that trains a neural network model to predict the future oxygen requirements of symptomatic patients with COVID-19, using inputs of vital signs, laboratory data, and chest X-rays [129]. An important fact to note is that, although federated learning allows for easy adoption, and resolves data privacy and security problems, it does not by itself ensure security and privacy except it is combined with other methods such as homomorphic encryption, differential privacy, and secure (multiparty) computation [127].

### 7.2. Cloud and blockchain privacy-preserving solutions: homomorphic encryption and differential privacy

In bioprinting, the 3D model utilized in the process will equate to an individual or patient's data. Large-scale data harnessed by AI models in the bioprinting ecosystem will be processed and outsourced on a powerful cloud-based server and this implies the possibility of significant data breaches. Considering the sensitive disposition of bioprinting data, all cloud storage and computing databases, applications, and software must be secure and private as required by law. Blockchain technology offers another innovative technique for storing bioprinting data and establishing trust in the bioprinting ecosystem. However, as discussed in section 3 above, it possesses shortcomings in terms of privacy and security challenges. In order to realize data privacy in the cloud and blockchain environment, a homomorphic encryption (HE) technique can be used to encrypt bioprinting data. HE entails the encryption of bioprinting data such that cloud users can compute/perform analysis on the bioprinting data as if it were in its original state [130]. An example of the application of HE as a cloud computing and blockchain privacy solution can be found in Ref. [131]. Their work proposes a homomorphic encryption based efficient, privacy-preserving algorithm called p-Impute that allows computations on ciphertext, therefore dispensing with the need for the decryption of private genotypes in the cloud. In summary, HE provides a safe avenue for private data to be retrieved from the bioprinting ecosystem and processed in the cloud. Differential privacy (DP) proves to be another technique for safeguarding bioprinting data that has been outsourced to blockchain or cloud computing services. Specifically, DP guarantees privacy irrespective of the intruders' knowledge of the bioprinting database. In particular, the approach in DP is to add artificial noise (Laplace or Gaussian) to an algorithm's output. The scale of noise is reliant on a privacy loss parameter ($\varepsilon$), which controls the amount of randomness or noise injected into the data, and sensitivity, which evaluates the effect of a change in the algorithms' input on the algorithm's output [131].

### 7.3. NextGen networks – TOR and onion routing

In the bioprinting ecosystem of the future, it is envisaged that the bioprinter will be fed sensitive patient or client data which will be transmitted to the cloud or to other machines via a Wi-Fi or 5G network interface. This data exchange between machines may be propagated through the internet, especially in cases when hospitals and their partner bioprinting labs are in separate and distant locations. This opens the network up to malicious attackers who can passively observe or monitor routing information and therefore plan a cyber-attack to siphon patient information. From a privacy and NextGen network standpoint, Tor onion routing presents an excellent solution for safeguarding data or information belonging to clients or end users in the bioprinting ecosystem. Onion routing was created by computer scientists and researchers working for the Naval Research Laboratory and Defense Advanced Research Projects Agency (DARPA) [132]. Onion routing can be used to protect user data in the bioprinting ecosystem by establishing multiple layers of encrypted connections to safeguard data from potential malicious attackers. Onion routing (aka Tor) is an open-source decentralized private network that constitutes thousands of voluntarily hosted servers [133]. It uses onion routing encryption to enable users to browse the internet anonymously. As its name implies, Tor onion routing works as follows: bioprinting data – such as the CAD model of a patient's tissue – transmitted by a user is the center of the "onion," and comprises the content of the message [134]. Upon incipient of the transmission process "by connecting to a Tor client, several layers of encryption surround the core, one atop the other like Russian nesting dolls, so that the core bioprinting data payload is inaccessible to outside actors" [161]. Tor offers anonymous connections that are greatly impervious to eavesdropping and traffic analysis.

## 8. Compliance, regulations, and standards

A cyber-secure bioprinting ecosystem offers various benefits such as allowing researchers to produce simple tissue constructs and complex scaffolds with spatial heterogeneity. However, this advent of this technology brings along certain expectations, especially in regard to the following.

### 8.1. Data privacy

When personal information is collected by the bioprinting ecosystem, care and consideration will be given in determining who (e.g., doctors, nurses, patients, etc.) maintains and controls the information and for what purposes it will be used [32]. One hurdle to overcome in bioprinting AI/ML implementation is that of compliance and regulations especially in relation to data and privacy laws. AI/ML service providers have to conform to demanding and rigorous data protection regulations such as the California Consumer Privacy Act (CCPA), the Brazilian General Data Protection Law (LGPD), and EU/UK General Data Protection Regulation (GDPR), and the proposed federal privacy law, the American Data Privacy Protection Act (ADPPA) – which is yet to be passed into law (as such, there is no comprehensive federal data privacy law in the U.S for now). However, on October 4, 2022, the White House released a set of guidelines to help lead the drive on companies limiting AI-based surveillance and deploying AI in a responsible manner [135].

### 8.2. Standards: zero trust architecture

The traditional network security approach is to readily trust all users, devices, and networks within the bioprinting ecosystems' perimeter: as long as any operation conducted within this perimeter has undergone appropriate authentication. However, this model places the bioprinting ecosystem at risk of unauthorized access by malicious agents and wide-reaching extensive system compromise. In addition, due to the heterogeneity of 5G networks, this model has become obsolete and has resulted in considerable cybersecurity issues [136]. Based on the foregoing, a "zero trust model which assumes no implicit trust granted to access or user accounts" is required [137]. NIST has recommended the adoption of a zero-trust architecture standard as a strategic approach to cybersecurity. This standard can be applied to the bioprinting ecosystem. A zero-trust architecture is a security framework that will require all exterior actors and actions (those existing outside the ecosystem's network) and interior users in the bioprinting ecosystem to be authenticated, authorized, and endlessly validated prior to gaining or maintaining access to the bioprinting ecosystem's applications, network and data [138]. A zero-trust network for the bioprinting ecosystems will work based on the following six tenets and assumptions [137]: 1) The network is always assumed to be hostile and should not be tacitly trusted. 2) Remote resources such as cloud services are not within the private network. 3) Remote/outsourced resources cannot fully trust their local network connection. 4) No resource should be fully trusted. 5) Users may connect external devices such as USBs to the network. These devices aren't owned or configurable by the organization. 6) Any asset or workflow that moves between internal and external infrastructure must have a consistent security posture.

### 8.3. Regulation

In 2021, President Biden issued an executive order [139] on improving the nation's cybersecurity. The nascent technology of a smart and cybersecure Bioprinting ecosystem presents a challenge to the nature of legal regulation. Bioprinted organs are regulated within the statutory purview of the FDA. Existing legal definitions permit bioprinted organs to be regulated under the "medical devices, biologics, drugs, or any combination of these three items'' classification [140]. However, according to Singh and Thomas [140], there is a problematic

sparsity when it comes to legal frameworks that provide guidance on the use of substances of human origin with nonliving materials". So far, the FDA has only provided guidelines for 3D printing, specifically, medical devices fabricated using 3D printing [6,141–144]. The National Institute of Standards and Technology (NIST) has presented a Cybersecurity Framework that can be adopted by any industry [145]. The zero-trust architecture standard which has been discussed in detail in the previous section represents a sub-aspect of this framework. In April 2022, the FDA issued a guideline titled "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket submissions" to assist the medical industry and healthcare organizations in detecting cybersecurity-related incidents that impact medical device functions and to promote awareness, preparedness, and responses for such incidents. Lastly, to promote transparency, the FDA publishes public communications about medical device cyber vulnerabilities that are acted on, could result in patient harm [146,147]. The FDA encourages medical device manufacturers to monitor and assess cybersecurity vulnerability risks, and to be proactive about divulging vulnerabilities and coming up with solutions to address them. It also maintains a database named "Manufacturer and User Facility Device Experience (MAUDE)" [148] that highlights the life-threatening dangers of medical device safety and security failures. However, a cursory search of the product class in the MAUDE database produces no results for bioprinters. Thus, ongoing cybersecurity strategies and evolving regulatory standards need to be explored in the biomanufacturing domain.

## 9. Open research and existing challenges

A cyber-secure smart bioprinting ecosystem offers various benefits such as allowing researchers to produce simple tissue constructs and complex scaffolds with spatial heterogeneity. However, the advent of this technology brings along certain expectations. In particular, it raises a number of questions that remain to be answered. These questions pertain mostly to privacy and security issues. The bioprinting ecosystem will utilize cellular data retrieved from patients. This attribute in conjunction with the use of IoT devices, AI/ML algorithms, cloud services, and NextGen networks to create a smart ecosystem leads to data privacy and security concerns. Data sharing is another unique feature of e-health systems [149], such as the smart bioprinting ecosystem. For instance, producing a custom-made implant using the smart bioprinting ecosystem will involve the extraction of patient data such as bioimages or CT scans. This data will be transmitted to the bioprinter, which is in turn monitored by sensors that transmit data to the cloud for research purposes, where it will be accessible to various stakeholders in the ecosystem such as doctors, hospitals, healthcare organizations, engineers, clinical data analysts/biostatisticians, cloud service companies, etc. The exchange of data between the ecosystem's stakeholders, especially for research intent, increases the number of people within a stakeholder group who have access to such data. This in turn increases the likelihood of data leakage and in a more serious case like a cyber-attack, a data breach. Another example is a case whereby cellular data extracted from a patient or donor is used and stored in the cloud. In the event of a data breach, patient data can be stolen and sold to third parties to be used in printing tissues for other patients across the world. Patients lose control over their data when it is stored in cloud servers, and this can be seen as a threat to patient privacy. Consequently, the who, how, and when of information sharing should entail the use of an adaptive access control model to oversee data exchange in the smart bioprinting ecosystem.

Given that smart bioprinting is currently in the early stages of development, there has been little to no attention paid to these concerns. Furthermore, privacy and security concerns also arise from the fact that in the distant future, bioprinting of transplantable tissues and organs will become more commonplace. As the technology develops, the latter the potential for tissues/organs to be tracked, hacked, and in more dire cases, controlled. For instance, an embedded sensor implanted in transplantable 3D printed blood vessels or in cardiac tissue for monitoring heartbeat or for detecting acute allograft rejection can be hacked to monitor and retrieve the transplant recipients' tissue information and release the same to the public, thus breaking HIPAA laws.

An additional aspect that needs to be explored in more detail is tissue construct quality/integrity. For example, in the event of a side-channel cyber-attack, a malicious actor can potentially hack the bioprinting ecosystem and alter the digital model to be used in printing the tissue/organ. This will have devastating consequences for transplant patients. It is imperative that a thorough in-cyber secure in-situ defect process in addition to post-printing quality inspection checks be set up to ensure that an organ is free from flaws or defects. In traditional 3D printing for example, researchers at Georgia Tech & Rutgers University developed a three-layer system made up of acoustic monitors, inexpensive microphones, detectable nanorods, and filtering software that detect changes in the usual sound a printer makes to tackle the issue of part integrity [150]. Based on the foregoing, it is crucial that security and data privacy concerns for the IoT-enabled smart bioprinting ecosystem be resolved before the technology becomes widely adopted by large biotech companies, the military, and other stakeholders.

## 10. Conclusion

Bioprinting technology signifies a novel area within the field of additive manufacturing. This technology is currently receiving intense attention in the research domain. Thus, making it appealing to various stakeholders that cut across manufacturing, healthcare, and other interrelated industries. This also demonstrates its huge potential for rapid evolution especially when integrated with the following technologies: AI/ML, cloud computing, NextGen networks, and blockchain to form a smart bioprinting ecosystem of the future. The integration of these technologies gives rise to myriad security challenges. This paper presents a multilayered architecture to illustrate the interaction between the aforementioned technologies in the smart bioprinting ecosystem. It also uses a layer-by-layer approach to highlight the cyber security challenges that may occur in the ecosystem. Another pertinent challenge that will arise from operating the bioprinting ecosystem is that of privacy, especially when taking into consideration that patient data will be collected, processed, and stored in the cloud. Consequently, the paper discusses privacy-preserving solutions for different facets of the ecosystem. It also touches on compliance, regulations, and standards involved in operating such an ecosystem, and finally, it provides a outlook on open research questions. The open research challenges discussed in this paper call for innovative scientific solutions that could probably be derived from conventional additive manufacturing research.

## Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Dr. Salil Desai reports financial support was provided by National Science Foundation.

## Data availability

No data was used for the research described in the article.

## Acknowledgement

The authors would like to express their gratitude for funding support from the National Science Foundation Grants (NSF Award #1663128, #2100739, #2100850, #2200538, #2113945), Carolina Cyber Network, Defense Manufacturing Community Support Program and the Center of Excellence in Product Design and Advanced Manufacturing at North Carolina A&T State University.

## References


[1] A.C. Daly, F.E. Freeman, T. Gonzalez-Fernandez, S.E. Critchley, J. Nulty, D. J. Kelly, 3D bioprinting for cartilage and osteochondral tissue engineering, Adv. Healthcare Mater. 6 (22) (Nov. 2017), 1700298, https://doi.org/10.1002/ADHM.201700298.

[2] G.J. Gillispie, et al., The Influence of Printing Parameters and Cell Density on Bioink Printing Outcomes, vol. 26, Dec. 2020, pp. 1349–1358, https://doi.org/10.1089/TEN.TEA.2020.0210. https://home.liebertpub.com/tea, 23–24.

[3] I. Matai, G. Kaur, A. Seyedsalehi, A. McClinton, C.T. Laurencin, Progress in 3D bioprinting technology for tissue/organ regenerative engineering, Biomaterials 226 (Jan. 2020), 119536, https://doi.org/10.1016/J.BIOMATERIALS.2019.119536.

[4] S.J. Trenfield, et al., Shaping the future: recent advances of 3D printing in drug delivery and healthcare 16 (10) (Oct. 2019) 1081–1094, https://doi.org/10.1080/17425247.2019.1660318, 10.1080/17425247.2019.1660318.

[5] H.W. Sanicola, et al., Guidelines for establishing a 3-D printing biofabrication laboratory, Biotechnol. Adv. 45 (Dec. 2020), 107652, https://doi.org/10.1016/J.BIOTECHADV.2020.107652.

[6] F.K. Aldawood, S.X. Chang, S. Desai, Design and manufacture of a high precision personalized electron bolus device for radiation therapy, Med. Devices Sensors 3 (6) (Dec. 2020), https://doi.org/10.1002/mds3.10077.

[7] E. Adarkwa, A. Roy, J. Ohodnicki, S. Desai, 3D printing of drug-eluting bioactive multifunctional coatings for orthopedic applications, Int. J. Bioprinting 110 (1) (Jul. 2023) [Online]. Available: https://www.ijb.sg/index.php/int-j-bioprinting.

[8] E. Adarkwa, R. Kotoka, S. Desai, 3D printing of polymeric Coatings on AZ31 Mg alloy Substrate for Corrosion Protection of biomedical implants, Med. Devices Sensors (Jan. 2021), https://doi.org/10.1002/mds3.10167.

[9] S. Vijayavenkataraman, W.C. Yan, W.F. Lu, C.H. Wang, J.Y.H. Fuh, 3D bioprinting of tissues and organs for regenerative medicine, Adv. Drug Deliv. Rev. 132 (Jul. 2018) 296–332, https://doi.org/10.1016/J.ADDR.2018.07.004.

[10] I. Marquetti, S. Desai, Nanoscale topographical effects on the adsorption behavior of bone morphogenetic protein-2 on graphite, Int. J. Mol. Sci. 23 (5) (Feb. 2022) 2432, https://doi.org/10.3390/IJMS23052432, 2022, Vol. 23, Page 2432.

[11] I. Marquetti, S. Desai, An atomistic investigation of adsorption of bone morphogenetic protein-2 on gold with nanoscale topographies, Surfaces 5 (1) (Feb. 2022) 176–185, https://doi.org/10.3390/SURFACES5010010, 2022, Vol. 5, Pages 176-185.

[12] I. Marquetti, S. Desai, Orientation effects on the nanoscale adsorption behavior of bone morphogenetic protein-2 on hydrophilic silicon dioxide, RSC Adv. 9 (2) (Jan. 2019) 906–916, https://doi.org/10.1039/C8RA09165J.

[13] I. Marquetti, S. Desai, Molecular modeling the adsorption behavior of bone morphogenetic protein-2 on hydrophobic and hydrophilic substrates, Chem. Phys. Lett. 706 (Aug. 2018) 285–294, https://doi.org/10.1016/j.cplett.2018.06.015.

[14] S. Kumar Parupelli, S. Saudi, N. Bhattarai, S. Desai, 3D printing of PCL-ceramic composite scaffolds for bone tissue engineering applications, Int. J. Bioprinting 9 (2) (Jul. 2023), https://doi.org/10.36922/ijb.0196, 0196.

[15] A. Shafiee, et al., Physics of bioprinting, Appl. Phys. Rev. 6 (2) (Jun. 2019), 021315, https://doi.org/10.1063/1.5087206.

[16] N. Almakayeel, S. Desai, S. Alghamdi, M.R. Noor, M. Qureshi, Smart agent system for cyber nano-manufacturing in industry 4.0, Appl. Sci. 12 (12) (Jun. 2022) 6143, https://doi.org/10.3390/APP12126143, 2022, Vol. 12, Page 6143.

[17] H. Elhoone, T. Zhang, M. Anwar, S. Desai, Cyber-based design for additive manufacturing using artificial neural networks for Industry 4.0, Int. J. Prod. Res. 58 (9) (May 2020) 2841–2861, https://doi.org/10.1080/00207543.2019.1671627.

[18] S. Desai, C. Dean, Y. Desai, Cyber-enabled concurrent material and process selection in a flexible design for manufacture paradigm, Int. J. Adv. Manuf. Technol. 97 (5–8) (Jul. 2018) 1719–1731, https://doi.org/10.1007/s00170-018-2034-6.

[19] M. Ogunsanya, S. Desai, Physics-based and data-driven modeling for biomanufacturing 4.0, Manuf. Lett. 36 (2023) 91–95, https://doi.org/10.1016/j.mfglet.2023.04.003.

[20] S. Desai, B. Bidanda, P.J. Bártolo, in: P.J. Bártolo, B. Bidanda (Eds.), Emerging Trends in the Applications of Metallic and Ceramic Biomaterials BT - Bio-Materials and Prototyping Applications in Medicine, Springer International Publishing, Cham, 2021, pp. 1–17, https://doi.org/10.1007/978-3-030-35876-1_1.

[21] S. Desai, M.R. Shankar, Emerging trends in polymers, composites, and nano biomaterial applications, in: Bio-Materials and Prototyping Applications in Medicine, Springer International Publishing, 2021, pp. 19–34, https://doi.org/10.1007/978-3-030-35876-1_2.

[22] M.H. Raza, S. Desai, S. Aravamudhan, R. Zadegan, An outlook on the current challenges and opportunities in DNA data storage, Biotechnol. Adv. 66 (Sep. 2023), 108155, https://doi.org/10.1016/J.BIOTECHADV.2023.108155.

[23] S. Thomas, 5 reasons cybersecurity will play a critical role in healthcare 3D printing. https://3dheals.com/cybersecurity-play-critical-role-healthcare-3d-printing, Feb. 23, 2019 accessed Jul. 19, 2021.

[24] M. Yampolskiy, et al., Security of additive manufacturing: attack taxonomy and survey, Addit. Manuf. 21 (May 2018) 431–457, https://doi.org/10.1016/J.ADDMA.2018.03.015.

[25] C. Dilmegani, Bias in AI: what it Is, Types, Examples & 6 Ways to Fix it in 2022, Feb. 09, 2022. https://research.aimultiple.com/ai-bias/. accessed Mar. 04, 2022.

[26] W. Sun, O. Nasraoui, P. Shafto, Evolution and impact of bias in human and machine learning algorithm interaction, PLoS One 15 (8) (Aug. 2020), e0235502, https://doi.org/10.1371/JOURNAL.PONE.0235502.

[27] N. Mehrabi, F. Morstatter, N. Saxena, K. Lerman, A. Galstyan, A survey on bias and fairness in machine learning, ACM Comput. Surv. 54 (6) (Jul. 2021), https://doi.org/10.1145/3457607.

[28] A. Parrott, L. Warshaw, Industry 4.0 and the Digital Twin Technology | Deloitte Insights," Deloitte Insights, May 12, 2017. https://www2.deloitte.com/us/en/insights/focus/industry-4-0/digital-twin-technology-smart-factory.html. accessed Jan. 19, 2023.

[29] M. Pantelidakis, K. Mykoniatis, J. Liu, G. Harris, A digital twin ecosystem for additive manufacturing using a real-time development platform, Int. J. Adv. Manuf. Technol. 120 (9–10) (Jun. 2022) 6547–6563, https://doi.org/10.1007/S00170-022-09164-6/FIGURES/15.

[30] H. Jiang and O. Nachum, "Identifying and Correcting Label Bias in Machine Learning." http://proceedings.mlr.press/v108/jiang20a.html (accessed Mar. 07, 2022)..

[31] M.B. Zafar, I. Valera, M.G. Rodriguez, K.P. Gummadi, Fairness beyond disparate treatment & disparate impact: learning classification without disparate mistreatment, in: 26th Int. World Wide Web Conf. WWW 2017, Oct. 2016, pp. 1171–1180, https://doi.org/10.1145/3038912.3052660.

[32] A.S. Elmaghraby, M.M. Losavio, Cyber security challenges in Smart Cities: safety, security and privacy, J. Adv. Res. 5 (4) (Jul. 2014) 491–497, https://doi.org/10.1016/J.JARE.2014.02.006.

[33] R. Schwartz, A. Vassilev, K. Greene, L. Perine, A. Burt, and P. Hall, "Towards a Standard for Identifying and Managing Bias in Artificial Intelligence," NIST Spec. Publ., p. 1270, doi: 10.6028/NIST.SP.1270..

[34] J. Dockès, G. Varoquaux, J.B. Poline, Preventing dataset shift from breaking machine-learning biomarkers, GigaScience 10 (9) (Sep. 2021) 1–11, https://doi.org/10.1093/GIGASCIENCE/GIAB055.

[35] J. Quionero-Candela, M. Sugiyama, Dataset Shift in Machine Learning, The MIT Press, 2009 [Online]. Available: https://dl.acm.org/doi/10.5555/1462129.

[36] H. Song, J.J. Thiagarajan, B. Kailkhura, Preventing failures by dataset shift detection in safety-critical graph applications, Front. Artif. Intell. 4 (May 2021) 60, https://doi.org/10.3389/FRAI.2021.589632/BIBTEX.

[37] J.G. Moreno-Torres, T. Raeder, R. Alaiz-Rodríguez, N.V. Chawla, F. Herrera, A unifying view on dataset shift in classification, Pattern Recogn. 45 (1) (Jan. 2012) 521–530, https://doi.org/10.1016/J.PATCOG.2011.06.019.

[38] D.S. Krueger, T. Maharaj, J. Leike, Hidden Incentives for Auto-Induced Distributional Shift, Sep. 2020, https://doi.org/10.48550/arxiv.2009.09153.

[39] R. Volpi, V. Murino, Addressing model vulnerability to distributional shifts over image transformation sets, in: Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV), 2019, pp. 7980–7989. Accessed: Mar. 14, 2022. [Online]. Available, https://openaccess.thecvf.com/content_ICCV_2019/html/Volpi_Addressing_Model_Vulnerability_to_Distributional_Shifts_Over_Image_Transformation_Sets_ICCV_2019_paper.html.

[40] D. Amodei, et al., Concrete Problems in AI Safety, Jun. 2016. Accessed: Feb. 24, 2022. [Online]. Available: https://arxiv.org/abs/1606.06565v2.

[41] X. Li, C.I. Vasile, C. Belta, Reinforcement learning with temporal logic rewards, IEEE Int. Conf. Intell. Robot. Syst. (Dec. 2017) 3834–3839, https://doi.org/10.1109/IROS.2017.8206234, 2017-September.

[42] B. Ibarz, G. Irving, J. Leike, S. Legg, T. Pohlen, D. Amodei, Reward learning from human preferences and demonstrations in Atari, Adv. Neural Inf. Process. Syst. 2018-December (Nov. 2018) 8011–8023. Accessed: Feb. 24, 2022. [Online]. Available: https://arxiv.org/abs/1811.06521v1.

[43] T. Everitt, M. Hutter, R. Kumar, V. Krakovna, Reward tampering problems and solutions in reinforcement learning: a causal influence diagram perspective, Synthese 198 (Aug. 2019) 6435–6467, https://doi.org/10.1007/s11229-021-03141-4.

[44] M. Alshiekh, R. Bloem, R. Ehlers, B. Könighofer, S. Niekum, U. Topcu, Safe reinforcement learning via shielding, in: 32nd AAAI Conf. Artif. Intell. AAAI 2018, Aug. 2017, pp. 2669–2678. Accessed: Feb. 28, 2022. [Online]. Available: https://arxiv.org/abs/1708.08611v2.

[45] A. Nazemi, P. Fieguth, Potential Adversarial Samples for White-Box Attacks, Dec. 2019, https://doi.org/10.48550/arxiv.1912.06409.

[46] N.G. Laleh, et al., Adversarial attacks and adversarial robustness in computational pathology, bioRxiv 7 (4) (Mar. 2022), https://doi.org/10.1101/2022.03.15.484515, 2022.03.15.484515.

[47] Y. Zhang, Y. Song, J. Liang, K. Bai, Q. Yang, Two sides of the same coin: white-box and black-box attacks for transfer learning, in: Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Min, vol. 20, Aug. 2020, pp. 2989–2997, https://doi.org/10.1145/3394486.3403349.

[48] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. Berkay Celik, A. Swami, Practical black-box attacks against machine learning, in: Proc. 2017 ACM Asia Conf. Comput. Commun. Secur, Apr. 2017, pp. 506–519, https://doi.org/10.1145/3052973.

[49] P.-Y. Chen, H. Zhang, Y. Sharma, J. Yi, C.-J. Hsieh, ZOO: zeroth order optimization based black-box attacks to deep neural networks without, Training Substitute Models 17 (2017), https://doi.org/10.1145/3128572.3140448.

[50] C. Guo, J.R. Gardner, Y. You, A.G. Wilson, K.Q. Weinberger, Simple black-box adversarial attacks, in: 36th Int. Conf. Mach. Learn. ICML 2019, May 2019, pp. 4410–4423, https://doi.org/10.48550/arxiv.1905.07121, 2019-June.

[51] S. Li, G. Huang, X. Xu, H. Lu, Query-based black-box attack against medical image segmentation model, Future Generat. Comput. Syst. 133 (Aug. 2022) 331–337, https://doi.org/10.1016/J.FUTURE.2022.03.008.

[52] H. Cao, S. Li, Y. Zhou, M. Fan, X. Zhao, Y. Tang, Towards Black-Box Attacks on Deep Learning Apps, Jul. 2021, https://doi.org/10.48550/arxiv.2107.12732.

[53] M.D. Champneys, A. Green, J. Morales, M. Silva, D. Mascarenas, 4, On the Vulnerability of Data-Driven Structural Health Monitoring Models to Adversarial Attack, vol. 20, May 2020, pp. 1476–1493, https://doi.org/10.1177/1475921720920233, 10.1177/1475921720920233.

[54] K. Lee, Improved Methodology for Evaluating Adversarial Robustness in Deep Neural Networks, Thesis: S.M., Massachusetts Institute of Technology, Department of Electrical Engineering and Computer Science, May 2020. https://dspace.mit.edu/handle/1721.1/127350. accessed May 02, 2022.

[55] Y. Zhang, P. Liang, Defending against whitebox adversarial attacks via randomized discretization, in: AISTATS 2019 - 22nd Int. Conf. Artif. Intell. Stat, Mar. 2019, https://doi.org/10.48550/arxiv.1903.10586.

[56] R. Pinot, et al., Theoretical evidence for adversarial robustness through randomization, Adv. Neural Inf. Process. Syst. 32 (Feb. 2019), https://doi.org/10.48550/arxiv.1902.01148.

[57] M. Melis, M. Pintor, A. Sotgiu, K. Murphy, B. Biggio, Secml: a Python library for secure and explainable machine learning, J. Mach. Learn. Res. 1 (Dec. 2019) 1–48, https://doi.org/10.48550/arxiv.1912.10013.

[58] B. Biggio, F. Roli, Wild patterns: ten years after the rise of adversarial machine learning, Pattern Recogn. 84 (Dec. 2018) 317–331, https://doi.org/10.1016/J.PATCOG.2018.07.023.

[59] F. Zhang, P.P.K. Chan, B. Biggio, D.S. Yeung, F. Roli, Adversarial feature selection against evasion attacks, IEEE Trans. Cybern. 46 (3) (Mar. 2016) 766–777, https://doi.org/10.1109/TCYB.2015.2415032.

[60] X. Cao, N.Z. Gong, Mitigating evasion attacks to deep neural networks via region-based classification, in: ACM Int. Conf. Proceeding Ser, Dec. 2017, pp. 278–287, https://doi.org/10.1145/3134600.3134606. Part F132521.

[61] A. Schwarzschild, M. Goldblum, A. Gupta, J.P. Dickerson, T. Goldstein, Just How Toxic Is Data Poisoning? A Unified Benchmark for Backdoor and Data Poisoning Attacks, Jun. 2020, https://doi.org/10.48550/arxiv.2006.12557.

[62] R.S. Siva Kumar, et al., Adversarial machine learning – industry perspectives, in: Proc. - 2020 IEEE Symp. Secur. Priv. Work. SPW 2020, Feb. 2020, pp. 69–75, https://doi.org/10.48550/arxiv.2002.05646.

[63] M. Goldblum, et al., Dataset Security for Machine Learning: Data Poisoning, Backdoor Attacks, and Defenses, Dec. 2020, https://doi.org/10.1109/TPAMI.2022.3162397.

[64] B. Biggio, B. Nelson, P. Laskov, Poisoning attacks against support vector machines, in: Proc. 29th Int. Conf. Mach. Learn. ICML 2012, vol. 2, Jun. 2012, pp. 1807–1814, https://doi.org/10.48550/arxiv.1206.6389.

[65] B. Nelson, et al., Exploiting Machine Learning to Subvert Your Spam Filter, 2008. Accessed: Apr. 01, 2022. [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/citations?doi=10.1.1.158.9598.

[66] A. Paudice, L. Muñoz-González, E.C. Lupu, Label sanitization against label flipping poisoning attacks, Lect. Notes Comput. Sci. (2019) 5–15, https://doi.org/10.1007/978-3-030-13453-2_1, 11329 LNAI.

[67] S. Shan, A.N. Bhagoji, H. Zheng, B.Y. Zhao, Traceback of Data Poisoning Attacks in Neural Networks, Oct. 2021, https://doi.org/10.48550/arxiv.2110.06904.

[68] F. Khoda Parast, C. Sindhav, S. Nikam, H. Izadi Yekta, K.B. Kent, S. Hakak, Cloud computing security: a survey of service-based models, Comput. Secur. 114 (Mar. 2022), 102580, https://doi.org/10.1016/J.COSE.2021.102580.

[69] J.L. Vázquez-Poletti, R. Moreno-Vozmediano, R. Han, W. Wang, I.M. Llorente, SaaS enabled admission control for MCMC simulation in cloud computing infrastructures, Comput. Phys. Commun. 211 (Feb. 2017) 88–97, https://doi.org/10.1016/J.CPC.2016.07.004.

[70] IBM, What Is PaaS (Platform-As-A-Service)? | IBM, Jul. 14, 2021. IBM.com, https://www.ibm.com/cloud/learn/paas?msclkid=007a8a50d0eb11ec88deb73151e5315b. (Accessed 11 May 2022).

[71] National Institute of Standards and Technology (NIST), P. Mell, T. Grance, The NIST definition of cloud computing recommendations of the national Institute of standards and technology, Natl. Inst. Stand. Technol. (2011), https://doi.org/10.6028/NIST.SP.800-145.

[72] V. Navale, P.E. Bourne, Cloud computing applications for biomedical science: a perspective, PLoS Comput. Biol. 14 (6) (Jun. 2018), e1006144, https://doi.org/10.1371/JOURNAL.PCBI.1006144.

[73] W. Wang, Data security of SaaS platform based on blockchain and decentralized technology, in: Proc. 5th Int. Conf. Inven. Comput. Technol. ICICT 2020, Feb. 2020, pp. 848–851, https://doi.org/10.1109/ICICT48043.2020.9112421.

[74] K. Hashizume, D.G. Rosado, E. Fernández-Medina, E.B. Fernandez, An analysis of security issues for cloud computing, J. Internet Serv. Appl. 4 (1) (Feb. 2013) 1–13, https://doi.org/10.1186/1869-0238-4-5/TABLES/4.

[75] B. Spasic, A.T. Rath, P. Thiran, N. Boucart, Security Pattern for Cloud SaaS: from system and data security to privacy, in: 2018 4th Int. Conf. Cloud Comput. Technol. Appl. Cloudtech 2018, Jul. 2018, https://doi.org/10.1109/CLOUDTECH.2018.8713339.

[76] J. Irvine, Encryption: what Does it Protect, what Are the Risks … and Is it Enough? - HS Today, Homeland Security Today, Jul. 13, 2015. https://www.hstoday.us/critical-issues-in-national-cybersecurity/encryption-what-does-it-protect-what-are-the-risks-and-is-it-enough/. (Accessed 17 May 2022).

[77] F. Office for Information Security, "Security Recommendations for Cloud Computing Providers," Fed. Off. Inf. Secur., Accessed: May 18, 2022. [Online] Available: www.bsi.bund.de.

[78] M.D. Aime, A. Lioy, P.C. Pomi, M. Vallini, Security plans for SaaS, Lect. Notes Bus. Inf. Process. (2011) 81–111, https://doi.org/10.1007/978-3-642-19294-4_4, 74 LNBIP.

[79] P.K. Chouhan, F. Yao, S. Sezer, Software as a service: understanding security issues, in: Proc. 2015 Sci. Inf. Conf. SAI 2015, Sep. 2015, pp. 162–170, https://doi.org/10.1109/SAI.2015.7237140.

[80] P.X. Wen, L. Dong, Quality model for evaluating SaaS service, in: Proc. - 4th Int. Conf. Emerg. Intell. Data Web Technol. EIDWT 2013, 2013, pp. 83–87, https://doi.org/10.1109/EIDWT.2013.19.

[81] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. 34 (1) (Jan. 2011) 1–11, https://doi.org/10.1016/J.JNCA.2010.07.006.

[82] J. Gao, X. Bai, W.T. Tsai, T. Uehara, SaaS testing on clouds - issues, challenges, and needs, in: Proc. - 2013 IEEE 7th Int. Symp. Serv. Syst. Eng. SOSE 2013, 2013, pp. 409–415, https://doi.org/10.1109/SOSE.2013.98.

[83] S.W. Boyd, A.D. Keromytis, SQLrand: preventing SQL injection attacks, Lect. Notes Comput. Sci. 3089 (2004) 292–302, https://doi.org/10.1007/978-3-540-24852-1_21/COVER.

[84] M. Jangjou, M.K. Sohrabi, A comprehensive survey on security challenges in different network layers in cloud computing, Arch. Comput. Methods Eng. 2022 (Jan. 2022) 1–22, https://doi.org/10.1007/S11831-022-09708-9.

[85] J. Gibson, R. Rondeau, D. Eveleigh, Q. Tan, Benefits and challenges of three cloud computing service models, in: Proc. 2012 4th Int. Conf. Comput. Asp. Soc. Networks, CASoN 2012, 2012, pp. 198–205, https://doi.org/10.1109/CASON.2012.6412402.

[86] E. Bauer, et al., Towards a security baseline for IaaS-cloud back-ends in Industry 4.0, in: 2017 12th Int. Conf. Internet Technol. Secur. Trans. ICITST 2017, May 2018, pp. 427–432, https://doi.org/10.23919/ICITST.2017.8356438.

[87] C. Modi, D. Patel, B. Borisaniya, A. Patel, M. Rajarajan, A survey on security issues and solutions at different layers of Cloud computing, J. Supercomput. 2012 632 63 (2) (Oct. 2012) 561–592, https://doi.org/10.1007/S11227-012-0831-5.

[88] Eclypsium, The Missing Security Primer for Bare Metal Cloud Services - Eclypsium, 2019. Accessed: Jul. 08, 2022. [Online]. Available: https://eclypsium.com/2019/01/26/the-missing-security-primer-for-bare-metal-cloud-services/.

[89] R. Badhwar, Man-in-the-Middle Attack Prevention, CISO's Next Front, 2021, pp. 223–229, https://doi.org/10.1007/978-3-030-75354-2_27.

[90] B. Subedi, A. Alsadoon, P.W.C. Prasad, A. Elchouemi, Secure paradigm for web application development, in: Netw. Educ. Res. RoEduNet Int. Conf. 15th Ed. RoEduNet 2016 - Proc, Nov. 2016, https://doi.org/10.1109/ROEDUNET.2016.7753243.

[91] T. Dillon, C. Wu, E. Chang, Cloud computing: issues and challenges, in: Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA, 2010, pp. 27–33, https://doi.org/10.1109/AINA.2010.187.

[92] M. Cloud Bu, Man in the cloud: threat, impact, resolution and the bigger picture | McAfee blog, McAfee.com (Aug. 21, 2015). https://www.mcafee.com/blogs/enterprise/cloud-security/man-in-the-cloud-threat-impact-resolution-and-the-bigger-picture/. (Accessed 6 June 2022).

[93] O. Garret, Trust No One: Trusting User Input Opens the Cloud Metadata Attack, NGINX, May 21, 2018. https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/. (Accessed 6 June 2022).

[94] R.N. Mitra, D.P. Agrawal, 5G mobile technology: a survey, ICT Express 1 (3) (Dec. 2015) 132–137, https://doi.org/10.1016/J.ICTE.2016.01.003.

[95] P. Pirinen, A brief overview of 5G research activities, in: Proc. 2014 1st Int. Conf. 5G Ubiquitous Connect. 5GU 2014, Feb. 2014, pp. 17–22, https://doi.org/10.4108/ICST.5GU.2014.258061.

[96] S. Sullivan, A. Brighente, S.A.P. Kumar, M. Conti, 5G security challenges and solutions: a review by OSI layers, IEEE Access 9 (2021) 116294–116314, https://doi.org/10.1109/ACCESS.2021.3105396.

[97] S. Zeb, A. Mahmood, S.A. Hassan, M.J. Piran, M. Gidlund, M. Guizani, Industrial digital twins at the nexus of NextG wireless networks and computational intelligence: a survey, J. Netw. Comput. Appl. 200 (Apr. 2022), 103309, https://doi.org/10.1016/J.JNCA.2021.103309.

[98] M.Z. Chowdhury, M.T. Hossan, M. Shahjalal, M.K. Hasan, Y.M. Jang, A new 5G eHealth architecture based on optical camera communication: an overview, prospects, and applications, IEEE Consum. Electron. Mag. 9 (6) (Nov. 2020) 23–33, https://doi.org/10.1109/MCE.2020.2990383.

[99] L. Chettri, R. Bera, A comprehensive survey on internet of things (IoT) toward 5G wireless systems, IEEE Internet Things J. 7 (1) (Jan. 2020) 16–32, https://doi.org/10.1109/JIOT.2019.2948888.

[100] M. Hassan, "Number of connected IoT devices growing 18% to 14.4 billion globally." https://iot-analytics.com/number-connected-iot-devices/(accessed Jul. 26, 2022)..

[101] F. Tettey, · Santosh, K. Parupelli, S. Desai, A review of biomedical devices: classification, regulatory guidelines, human factors, software as a medical device, and cybersecurity, Biomed. Mater. Devices 2023 1 (Aug. 2023) 1–26, https://doi.org/10.1007/S44174-023-00113-9.

[102] Y. Wu, V.L. Vida, M. Zheng, J. Yang, Progress and prospects of cardiovascular 3D printing, Cardiovasc. 3D Print. (2021) 179–185, https://doi.org/10.1007/978-981-15-6957-9_13.

[103] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, A. Gurtov, 5G security: analysis of threats and solutions, in: 2017 IEEE Conf. Stand. Commun. Networking, CSCN 2017, Oct. 2017, pp. 193–199, https://doi.org/10.1109/CSCN.2017.8088621.

[104] Y. Shi, Y.E. Sagduyu, T. Erpek, M.C. Gursoy, How to Attack and Defend 5G Radio Access Network Slicing with Reinforcement Learning, Jan. 2021, https://doi.org/10.48550/arxiv.2101.05768.

[105] H. Pirayesh, H. Zeng, Jamming attacks and anti-jamming strategies in wireless networks: a comprehensive survey, IEEE Commun. Surv. Tutorials 24 (2) (2022) 767–809, https://doi.org/10.1109/COMST.2022.3159185.

[106] Y. Arjoune, S. Faruque, Smart jamming attacks in 5G new radio: a review, in: 2020 10th Annu. Comput. Commun. Work. Conf. CCWC 2020, Jan. 2020, pp. 1010–1015, https://doi.org/10.1109/CCWC47524.2020.9031175.
[107] A. Dutta, E. Hammad, 5G security challenges and opportunities: a system approach, in: 2020 IEEE 3rd 5G World Forum, 5GWF 2020 - Conf. Proc., Sep. 2020, pp. 109–114, https://doi.org/10.1109/5GWF49715.2020.9221122.
[108] B. Alhijawi, S. Almajali, H. Elgala, H. Bany Salameh, M. Ayyash, A survey on DoS/DDoS mitigation techniques in SDNs: classification, comparison, solutions, testing tools and datasets, Comput. Electr. Eng. 99 (Apr. 2022), 107706, https://doi.org/10.1016/J.COMPELECENG.2022.107706.
[109] N.A.E. Kuadey, G.T. Maale, T. Kwantwi, G. Sun, G. Liu, DeepSecure: detection of distributed denial of service attacks on 5G network slicing - deep learning approach, IEEE Wirel. Commun. Lett. 11 (3) (Mar. 2022) 488–492, https://doi.org/10.1109/LWC.2021.3133479.
[110] S. Nakamoto, Bitcoin P2P e-cash paper, Metzdowd.com, https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html, Oct. 31, 2008. (Accessed 1 August 2022).
[111] D. Tse, B. Zhang, Y. Yang, C. Cheng, H. Mu, Blockchain application in food supply information security, in: IEEE Int. Conf. Ind. Eng. Eng. Manag, Feb. 2018, pp. 1357–1361, https://doi.org/10.1109/IEEM.2017.8290114, 2017-December.
[112] U. Bodkhe, et al., Blockchain for Industry 4.0: a comprehensive review, IEEE Access 8 (2020) 79764–79800, https://doi.org/10.1109/ACCESS.2020.2988579.
[113] J. Lee, M. Azamfar, J. Singh, A blockchain enabled Cyber-Physical System architecture for Industry 4.0 manufacturing systems, Manuf. Lett. 20 (Apr. 2019) 34–39, https://doi.org/10.1016/J.MFGLET.2019.05.003.
[114] T. McGhin, K.K.R. Choo, C.Z. Liu, D. He, Blockchain in healthcare applications: research challenges and opportunities, J. Netw. Comput. Appl. 135 (Jun. 2019) 62–75, https://doi.org/10.1016/J.JNCA.2019.02.027.
[115] M. Gupta, M. Abdelsalam, S. Khorsandroo, S. Mittal, Security and privacy in smart farming: challenges and opportunities, IEEE Access 8 (2020) 34564–34584, https://doi.org/10.1109/ACCESS.2020.2975142.
[116] B. Mackenzie, R.I. Ferguson, X. Bellekens, An assessment of blockchain consensus protocols for the internet of things, in: 2018 Int. Conf. Internet Things, Embed. Syst. Commun. IINTEC 2018 - Proc., Jul. 2018, pp. 183–190, https://doi.org/10.1109/IINTEC.2018.8695298.
[117] M. Klöckner, S. Kurpjuweit, C. Velu, S.M. Wagner, Does Blockchain for 3D Printing Offer Opportunities for Business Model Innovation? 63 (4) (Jul. 2020) 18–27, https://doi.org/10.1080/08956308.2020.1762444, 10.1080/08956308.2020.1762444.
[118] Z.C. Kennedy, et al., Enhanced anti-counterfeiting measures for additive manufacturing: coupling lanthanide nanomaterial chemical signatures with blockchain technology, J. Mater. Chem. C 5 (37) (Sep. 2017) 9570–9578, https://doi.org/10.1039/C7TC03348F.
[119] M. Holland, J. Stjepandic, C. Nigischer, Intellectual property protection of 3D print supply chain with blockchain technology, in: 2018 IEEE Int. Conf. Eng. Technol. Innov. ICE/ITMC 2018 - Proc., Aug. 2018, https://doi.org/10.1109/ICE.2018.8436315.
[120] T. Ghimire, A. Joshi, S. Sen, C. Kapruan, U. Chadha, S.K. Selvaraj, Blockchain in additive manufacturing processes: recent trends & its future possibilities, Mater. Today Proc. 50 (Jan. 2022) 2170–2180, https://doi.org/10.1016/J.MATPR.2021.09.444.
[121] C. Mandolla, A.M. Petruzzelli, G. Percoco, A. Urbinati, Building a digital twin for additive manufacturing through the exploitation of blockchain: a case analysis of the aircraft industry, Comput. Ind. 109 (Aug. 2019) 134–152, https://doi.org/10.1016/J.COMPIND.2019.04.011.
[122] S. Asiri, A. Miri, A sybil resistant IoT trust model using blockchains, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Jul. 2018, pp. 1017–1026, https://doi.org/10.1109/Cybermatics_2018.2018.00190.
[123] P. Otte, M. de Vos, J. Pouwelse, TrustChain: a Sybil-resistant scalable blockchain, Future Generat. Comput. Syst. 107 (Jun. 2020) 770–780, https://doi.org/10.1016/J.FUTURE.2017.08.048.
[124] K. Wang, Y. Wang, Z. Ji, Defending blockchain forking attack by delaying MTC confirmation, IEEE Access 8 (2020) 113847–113859, https://doi.org/10.1109/ACCESS.2020.3000571.
[125] S. Barber, X. Boyen, E. Shi, E. Uzun, Bitter to better - how to make bitcoin a better currency, Lect. Notes Comput. Sci. (2012) 399–414, https://doi.org/10.1007/978-3-642-32946-3_29/COVER, 7397 LNCS.
[126] F. Alkurdi, I. Elgendi, K.S. Munasinghe, D. Sharma, A. Jamalipour, Blockchain in IoT security: a survey, in: 2018 28th Int. Telecommun. Networks Appl. Conf. ITNAC 2018, Jan. 2019, https://doi.org/10.1109/ATNAC.2018.8615409.
[127] B. McMahan, E. Moore, D. Ramage, S. Hampson, B.A. y Arcas, Communication-efficient learning of deep networks from decentralized data, in: Proceedings of Machine Learning Research, Apr. 2017, pp. 1273–1282. Accessed: Oct. 29, 2022. [Online]. Available: https://proceedings.mlr.press/v54/mcmahan17a.html.
[128] D. Enthoven, Z. Al-Ars, An overview of federated deep learning privacy attacks and defensive strategies, Stud. Comput. Intell. 965 (Apr. 2020) 173–196, https://doi.org/10.48550/arxiv.2004.04676.
[129] I. Dayan, et al., Federated learning for predicting clinical outcomes in patients with COVID-19, Nat. Med. 27 (10) (Sep. 2021) 1735–1743, https://doi.org/10.1038/s41591-021-01506-3, 2021 2710.
[130] F. Armknecht, et al., A Guide to Fully Homomorphic Encryption, Cryptol. ePrint Arch., 2015.
[131] H. Wang, Q. Zhao, Q. Wu, S. Chopra, A. Khaitan, H. Wang, Global and local differential privacy for collaborative bandits, in: RecSys 2020 - 14th ACM Conf. Recomm. Syst, vol. 20, Sep. 2020, pp. 150–159, https://doi.org/10.1145/3383313.3412254.
[132] R. Dingledine, N. Mathewson, P. Syverson, "Tor: the Second-Generation Onion Router," Washington DC, Jan. 2004. Nov. 25, 2022. [Online]. Available, https://apps.dtic.mil/sti/citations/ADA465464.
[133] E. Eaton, S. Sasy, I. Goldberg, Improving the privacy of tor onion services, Lect. Notes Comput. Sci. (2022) 273–292, https://doi.org/10.1007/978-3-031-09234-3_14/COVER, 13269 LNCS.
[134] K. Swan, Onion routing and tor, Georg. Law Technol. Rev. 1 (2016) 110–118. Nov. 25, 2022. [Online]. Available: https://heinonline.org/HOL/Page?handle=hein.journals/gtltr1&id=110&div=15&collection=journals.
[135] Office of the President, "Blueprint for an AI Bill of Rights - OSTP - The White House." https://www.whitehouse.gov/ostp/ai-bill-of-rights/(accessed Oct. 31, 2022).
[136] C. Rong, J. Geng, T.J. Hacker, H. Bryhni, M.G. Jaatun, OpenIaC: open infrastructure as code - the network is my computer, J. Cloud Comput. 11 (1) (Dec. 2022) 1–13, https://doi.org/10.1186/S13677-022-00285-7/FIGURES/7.
[137] S. Rose, O. Borchert, S. Mitchell, S. Connelly, Zero trust architecture, NIST Comput. Secur. Resour. Cent. (Aug. 2020), https://doi.org/10.6028/NIST.SP.800-207.
[138] A. Kerman, O. Borchert, S. Rose, E. Division, A. Tan, Implementing a zero trust architecture, 17–17, NIST Comput. Secur. Resour. Cent. (Oct. 2020). Accessed: Nov. 27, 2022. [Online]. Available: https://csrc.nist.gov/publications/detail/white-paper/2020/10/21/implementing-a-zero-trust-architecture/final.
[139] J.R. Biden Jr., Executive Order on Improving the Nation's Cybersecurity | the White House, The White House Briefing Room, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/. accessed Oct. 12, 2022.
[140] D. Singh, D.J. Thomas, Regulation and safety, 3D Print. Med. Surg. Appl. Healthc. (Jan. 2021) 271–275, https://doi.org/10.1016/B978-0-08-102542-0.00014-2.
[141] FDA, FDA's role in 3D printing | FDA, US Food & Drug Admininstration (Dec. 04, 2017). https://www.fda.gov/medical-devices/3d-printing-medical-devices/fdas-role-3d-printing. Oct. 12, 2022.
[142] F. Khaled Aldawood, A. Andar, S. Desai, G. Giammona, E. Fabiola Craparo, A comprehensive review of microneedles: types, materials, processes, characterizations and applications, Polym 13 (16) (Aug. 2021) 2815, https://doi.org/10.3390/POLYM13162815, 2021, Vol. 13, Page 2815.
[143] M. Olowe, S.K. Parupelli, S. Desai, A review of 3D-printing of microneedles, Pharm. Times 14 (12) (Dec. 2022) 2693, https://doi.org/10.3390/PHARMACEUTICS14122693, 2022, Vol. 14, Page 2693.
[144] S. Desai, S.K. Parupelli, Maynard's Industrial and Systems Engineering Handbook, Sixth Edition Chapter: 60 Additive Manufacturing, 2022, pp. 1175–1206.
[145] NIST, "NIST Cybersecurity Framework | NIST." https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework (accessed Oct. 23, 2022)..
[146] US Food and Drug Administration. Premarket Approval (PMA), Infuse bone graft/lt-cage lumbar tapered fusion device. . https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpma/pma.cfm?id=P000058 (accessed Jan. 19, 2022)..
[147] N.M. Thomasian, E.Y. Adashi, Cybersecurity in the internet of medical things, Heal. Policy Technol. 10 (3) (Sep. 2021), 100549, https://doi.org/10.1016/J.HLPT.2021.100549.
[148] US Food & Drug Administration, "MAUDE - Manufacturer and User Facility Device Experience." https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/Search.cfm?smc=1 (accessed Nov. 28, 2022)..
[149] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, Security and privacy-preserving challenges of e-health solutions in cloud computing, IEEE Access 7 (2019) 74361–74382, https://doi.org/10.1109/ACCESS.2019.2919982.
[150] J. O'Heir, Protecting a New World of 3D-Printed Products, The American Society of Mechanical Engineers, Jan. 25, 2018. https://www.asme.org/topics-resources/content/protecting-new-world-3dprinted-products. accessed Nov. 21, 2022.