

3D-Animated Digital Twins in the Metaverse: Security Challenges, Ethical Risks, and Societal Implications

Priyanka Priyadarshini^{1,*}, Tarakanta Sahoo²

Abstract

Metaverse is emerging as an immersive digital space where users interact through virtual environments. Within this space, 3D-animated digital twins act as virtual representations of real individuals, objects, and systems, enabling interaction, simulation, and presence beyond physical boundaries. While these digital replicas provide significant opportunities for engagement and innovation, they also raise critical security and ethical concerns. Security vulnerabilities can lead to identity misuse, impersonation, and unauthorized access, threatening personal safety and trust in virtual platforms. Ethical challenges include issues of consent, ownership, and privacy, particularly when digital twins closely resemble real individuals. Misuse of these representations can result in identity distortion, psychological harm, and social disruption, affecting not only individuals but also communities and institutional credibility. The absence of clear governance frameworks may amplify these risks, creating conflicts between technological capabilities and societal values. This paper adopts a non-technical, interdisciplinary approach that emphasizes ethical awareness, responsible practices, and policy-based safeguards. It explores how security and ethics are interconnected and how addressing both is essential to sustain trust, equity, and inclusion in virtual spaces. By linking technical risks with societal implications, the study highlights the importance of proactive management to prevent harm and ensure accountability. Ultimately, the responsible deployment of digital twins is crucial to unlocking their potential while maintaining safe, ethical, and socially inclusive metaverse environments. Early consideration of these challenges is vital for promoting long-term digital well-being.

Keywords: Metaverse, twins, security, ethics, identity, society

INTRODUCTION

The metaverse is an emerging digital environment in which individuals interact, collaborate, and experience spaces beyond physical limits. Unlike traditional online platforms, it allows users to navigate and engage through virtual representations, creating a sense of presence and co-existence in shared spaces [1]. Within this space, 3D-animated digital twins are increasingly used to represent real-world entities. These twins can simulate the behavior of people, objects, or systems, enabling interaction, learning, and experimentation in a controlled digital environment [2]. Digital twins enhance immersion and allow users to explore scenarios that may be difficult or risky in the real world. In education, they enable students to participate in virtual laboratories or simulations that mimic real-life experiments. In healthcare, they support patient-specific modelling and remote treatment planning, improving accessibility and safety [3]. Similarly, businesses and urban planners use digital twins to model processes, test designs, and improve operational efficiency [4].

*Author for Correspondence

Priyanka Priyadarshini

E-mail: pp.priyadarshini12345@gmail.com

¹Assistant Professor, Department of Basic Science and Humanities, Gandhi Institute of Excellent Technocrats, Ghangapatna, Bhubaneswar, Odisha, India

²Professor & HoD, Department of Basic Science and Humanities, Gandhi Institute of Excellent Technocrats, Ghangapatna, Bhubaneswar, Odisha, India

Received Date: January 27, 2026

Accepted Date: February 01, 2026

Published Date: February 04, 2026

Citation: Priyanka Priyadarshini, Tarakanta Sahoo. 3D-Animated Digital Twins in the Metaverse: Security Challenges, Ethical Risks, and Societal Implications. Journal of Network Security. 2026; 14(2): 11–19p.

Although these tools offer significant benefits, they also raise serious concerns. Security risks, such as identity misuse, data breaches, and unauthorized manipulation, can compromise personal safety and trust [5]. Ethical challenges arise when digital twins replicate real individuals, raising questions regarding consent, ownership, and accountability. The misuse of these virtual representations can affect not only the individuals involved but also broader social norms and interactions. Additionally, unequal access to digital twins may amplify digital inequality, creating gaps in education, healthcare, and professional opportunities for some students. Addressing these challenges requires careful attention to policies, governance, and ethical guidelines. This study examines the security challenges, ethical risks, and societal implications of 3D-animated digital twins in the metaverse. It emphasizes a non-technical, interdisciplinary approach to understanding these issues. By highlighting both the potential and risks, this study aims to provide insights into how digital twins can be responsibly developed and managed to ensure safe, ethical, and socially meaningful use in emerging virtual environments.

THEORETICAL FRAMEWORK

This study is grounded in sociotechnical and ethical frameworks, emphasizing the interplay between technology, society, and human values [6, 7]. The metaverse functions as a complex sociotechnical system in which 3D-animated digital twins serve as extensions of real-world entities, shaping social interactions, identity representation, and decision-making processes. Technology is not neutral; its design, deployment, and use reflect social norms, ethical principles, and regulatory contexts [8]. Therefore, digital twins are analyzed as both technological artifacts and instruments with societal influence, affecting privacy, trust, and equity. Ethical frameworks provide a foundation for examining the responsible creation and use of digital twins. The principles of autonomy, consent, fairness, and accountability guide the assessment of potential risks, including unauthorized identity replication, data misuse, and unequal access [9]. By applying ethical considerations, this study evaluates not only the technical functionalities but also the broader social and moral consequences of digital twin deployment in the metaverse.

Sociocultural theories of trust and social capital further inform this study's framework. Trust is critical for user engagement, collaboration, and adoption in immersive digital environments, whereas social capital influences community cohesion and equitable participation [10]. Digital twins can enhance or disrupt these dynamics, depending on how they are managed and perceived by users. Finally, sociotechnical systems theory underlines the interdependence between technology, human actors, and organizational structures, highlighting that responsible innovation requires simultaneous attention to technical design, social practices, and governance [11]. Integrating sociotechnical, ethical, and sociocultural perspectives enables a holistic understanding of digital twins, examining how they impact users, communities, and societal norms, while guiding strategies for responsible and inclusive adoption [12].

FUNCTIONALITY AND POTENTIAL OF 3D TWINS

Digital twins are virtual replicas of real-world entities that mirror their structure, behavior, and functionality in a digital environment [13]. In the metaverse, these twins are 3D-animated, meaning they are interactive, visually immersive, and capable of responding to changes in real time [14]. Unlike static models, 3D digital twins can simulate movement, interactions, and environmental changes, creating a sense of realism and presence for users [15]. This interactivity makes them valuable tools for education, healthcare, industry, and social interactions. Initially, digital twins were developed in engineering and manufacturing to monitor machinery, predict failures, and optimize performance without physical risks [16]. Over time, the concept expanded into social and digital spaces, allowing digital twins to represent people, organizations, and processes in the metaverse [17]. These twins are not only functional models but also symbolic representations of their identities. They allow individuals to project themselves into immersive environments, bridging the physical and digital worlds of the metaverse.

The applications of 3D digital twins in the metaverse are varied. In education, they facilitate virtual labs, interactive lessons, and safe simulations for experimentation [5]. In healthcare, they provide patient-specific models, simulate treatments, and support remote monitoring, thereby improving accuracy and reducing risk [13]. Businesses use digital twins to optimize operations, test strategies, and predict outcomes before implementing changes in the real world [16]. In urban planning, entire cities can be recreated as digital twins to model traffic flows, environmental changes, and public safety measures [17]. The importance of 3D-animated digital twins lies in their ability to enhance decision-making, collaboration, and innovation. They also enable remote interaction, which is critical in a globally connected environment in which physical presence is not always possible [15]. However, as digital twins increasingly mirror real-world identities, their use raises ethical and security concerns that must be addressed. Ownership, consent, and privacy are central issues, as misuse can have real-world consequences. Therefore, understanding the functionality and applications of digital twins is essential for exploring both their benefits and the risks they pose in the metaverse [18].

GUARDING THE VIRTUAL FRONTIER: SECURITY RISKS AND VULNERABILITIES

As 3D-animated digital twins become increasingly integrated into the metaverse, they face multiple security challenges that can compromise both personal and organizational safety. These twins often contain sensitive data, including personal identifiers, behavioral patterns, and real-time activity logs, making them prime targets for cyberattacks [19]. Unauthorized access to digital twins can lead to identity theft, impersonation, or manipulation of virtual representations. Such incidents not only threaten individuals' privacy but can also damage social trust and institutional credibility. One major concern is the compromise of identity. Because digital twins closely mirror real people, attackers can exploit them for fraudulent activities, social engineering, or reputation damage [20]. Virtual impersonation in the metaverse can be difficult to detect because of the immersive and interactive nature of 3D twins, increasing the risk of deception. Similarly, data breaches can expose private information, including biometrics, personal preferences, and location data, raising legal and ethical concerns regarding consent and accountability [21]. Another challenge is the unauthorized manipulation of the data. Hackers or malicious users can modify the behavior or appearance of digital twins to mislead others, simulate false interactions, or disrupt collaborative environments [22]. Such manipulation can undermine professional simulations, educational exercises, or healthcare modelling, producing real-world consequences.

Additionally, the interconnectedness of digital twins within the metaverse amplifies their vulnerabilities. A compromised twin can affect the linked systems, causing cascading effects across networks and platforms. Security concerns are compounded by insufficient governance and regulations. Current frameworks often lag behind technological advances, leaving users and organizations exposed [19]. The dynamic nature of the metaverse, where digital twins are constantly updated and modified, creates challenges in monitoring access, authenticating users, and enforcing security policies. To mitigate these risks, stakeholders must implement a combination of technical, policy, and awareness-based strategies. Although technical solutions such as encryption, authentication protocols, and monitoring are essential, they must be complemented by ethical policies, user education, and governance frameworks to ensure the responsible and secure use of digital twins in immersive environments [20]. Proactively addressing security challenges is critical for preserving the integrity of digital twins and maintaining trust in the metaverse. Failure to do so could undermine the potential benefits and societal acceptance of immersive digital technologies.

MORAL CONSIDERATIONS FOR DIGITAL TWINS

The increasing realism of 3D-animated digital twins in the metaverse introduces several ethical risks that extend beyond technical concerns of the technology. One primary issue is consent. Individuals may not fully understand how their digital twin is created, used, or shared, raising questions about informed consent and personal autonomy [9]. Digital twins that replicate behaviors, appearances, or personal data without clear consent can violate privacy and trust. Ownership is another critical issue. When digital

twins mirror individuals, it is often unclear who legally or ethically controls them. Users, developers, and platforms may all claim partial rights, creating conflicts over access, modification, and usage [23]. The mismanagement of ownership rights can result in misuse, unauthorized replication, or monetization of digital representations without the individual's knowledge.

The ethical implications of identity and representation are also significant in this context. Digital twins can exaggerate, distort, or misrepresent aspects of a person's identity, potentially leading to psychological harm or social misperception [24]. For example, manipulated twins could be used to spread misinformation or harass individuals, undermining trust in virtual communities. Similarly, digital inequality arises when access to advanced twin technologies is limited by socioeconomic status, geography, or digital literacy, exacerbating existing societal disparities [25]. Accountability is another concern. When actions are performed by or through a digital twin, determining responsibility for errors, harm, or misconduct becomes complicated. The misuse of digital twins in educational, healthcare, or professional contexts can have real-world consequences; however, existing frameworks rarely provide clear guidance [26–28].

To address these ethical challenges, developers and policymakers must adopt transparent, fair, and socially responsible principles. Users should be informed about the data collection, use, and representation of their digital twins. Guidelines for ownership, modification, and access must be established to protect individual rights. Additionally, ethical awareness programs and digital literacy initiatives can empower users to navigate virtual environments safely and responsibly [9]. Ultimately, the ethical management of 3D-animated digital twins is critical for fostering trust, inclusion, and fairness in the metaverse. Without clear ethical frameworks, the adoption of these technologies could harm individuals and communities, thereby limiting the societal benefits of immersive virtual experiences.

SOCIETAL IMPLICATIONS OF DIGITAL TWINS IN THE METAVERSE

The integration of 3D-animated digital twins in the metaverse has profound societal implications that extend beyond individual users. One major impact is social interaction. Although digital twins enable immersive communication and collaboration, they can also blur the line between real and virtual identities [29]. Users may engage with avatars that misrepresent their intentions or emotions, affecting trust and social cohesion in both virtual and real-world communities. Another implication is the psychological impact. The ability to project an idealized or manipulated digital twin can influence self-perception, body image, and social confidence of the user. Extended interaction with digital twins may also contribute to dependency on virtual validation, affecting mental well-being and personal relationships.

Work and education have also been transformed by digital twins. In professional environments, twins enable remote training, workflow simulation, and collaborative design across locations. While these tools enhance efficiency and accessibility, they may inadvertently create inequalities if some individuals lack access to advanced metaverse technologies [30]. Similarly, in education, digital twins provide interactive learning experiences but may widen the gaps between well-resourced and under-resourced institutions. Digital twins also raise ethical and cultural concerns at the societal level. The misuse of twins for misinformation, identity manipulation, or digital harassment can damage reputation and social trust [31]. Communities must develop norms and policies to govern acceptable behavior and protect vulnerable populations from exploitation and exclusion.

Furthermore, digital twins have policy and governance implications. Governments, organizations, and platform developers must address the legal frameworks surrounding data privacy, ownership, and accountability. The societal adoption of digital twins depends on transparent regulations and ethical guidelines that balance innovation and public safety [26]. In conclusion, the societal implications of 3D-animated digital twins are complex and multidimensional. They can enhance interaction, collaboration, and learning, but they also introduce challenges in terms of trust, equity, and ethical

governance. Recognizing these implications is essential to guide the responsible development, adoption, and management of digital twins in the metaverse, ensuring that they contribute positively to both virtual and real-world communities.

BUILDING TRUST: APPROACHES TO RESPONSIBLE AND SAFE TWIN DEPLOYMENT

The widespread adoption of 3D-animated digital twins in the metaverse requires comprehensive strategies that address security, ethics, and social responsibility. Ensuring user protection and maintaining trust in virtual environments requires attention to both technical and non-technical aspects. By combining robust safeguards, transparent governance, digital literacy initiatives, interdisciplinary collaboration, and clear policy frameworks, stakeholders can effectively reduce the risks and uphold ethical standards. Thoughtful management of digital twins promotes a safe, inclusive, and reliable metaverse, enabling users to engage in immersive experiences while safeguarding their privacy, autonomy, and well-being.

1. *Robust data protection*: Digital twins often contain personal, behavioral, or organizational data, making encryption, secure storage, and controlled access essential [32]. Platforms should implement authentication measures to prevent unauthorized access and ensure that sensitive information remains confidential. Regular audits and monitoring of data flow can further reduce security risks.
2. *Ethical governance*: Developers and platform managers must establish clear policies regarding consent, ownership, and the permissible uses of digital twins [33]. Users should be informed about how their digital twins are created, shared, and modified. Transparent guidelines help prevent misuse, unauthorized replication, and exploitation while promoting trust between users and platforms.
3. *Digital literacy and awareness*: Educating users about potential risks, ethical considerations, and safe practices empowers individuals to make informed decisions in the metaverse [34]. Training programs can help users understand data privacy, recognize manipulation, and adopt responsible interaction norms.
4. *Interdisciplinary collaboration*: Combining expertise from technology, ethics, law, and social sciences enables the development of comprehensive policies and frameworks that address both security and societal concerns [35, 32]. This collaboration ensures that the deployment of digital twins considers the practical, ethical, and social dimensions.
5. *Regulatory and policy frameworks*: Governments and organizations must create laws that define ownership, liability, and accountability for digital representations [36]. Compliance with these frameworks, combined with self-regulatory industry standards, helps protect users and support ethical innovations.

LESSONS FROM REAL-WORLD APPLICATIONS

Several real-world applications of 3D-animated digital twins illustrate their potential and challenges associated with their use in the metaverse. A notable example is the digital twin platform for industrial operations. Siemens creates digital replicas of factories to simulate production processes, optimize efficiency, and predict machine failures. Although the platform has improved operational decision-making, it has also highlighted security risks, including unauthorized access to sensitive industrial data, emphasizing the need for robust cybersecurity measures [16]. In healthcare, the Philips Virtual Hospital project uses digital twins of patients to simulate treatment plans and remotely monitor responses. This approach enhances personalized care and reduces medical errors. However, this raises ethical concerns regarding patient consent, data privacy, and ownership of digital health data, demonstrating the importance of ethical governance alongside technological innovation [3].

Another example is Singapore's Virtual Twin City project, which recreates the urban environment as a 3D digital twin for planning traffic flows, energy management, and disaster preparedness purposes. The project provides valuable applications of 3D digital twins in the metaverse are varied. In education, they facilitate virtual labs, interactive lessons, and safe simulations for experimentation [5]. In healthcare, they provide patient-specific models, simulate treatments, and support remote monitoring,

thereby improving accuracy and reducing risk [13]. Businesses use digital twins to optimize operations, test strategies, and predict outcomes before implementing changes in the real world [16]. Even in urban planning, entire cities can be recreated as digital twins to model traffic flow, environmental changes, and public safety measures [17]. The importance of 3D-animated digital twins lies in their ability to enhance decision-making, collaboration, and innovation. They also enable remote interaction, which is critical in a globally connected environment in which physical presence is not always possible [15]. However, as digital twins increasingly mirror real-world identities, their use raises ethical and security concerns that must be addressed. Ownership, consent, and privacy are central issues, as misuse can have real-world consequences. Therefore, understanding the functionality and applications of digital twins is essential for exploring both their benefits and the risks they pose in the metaverse.

GUARDING THE VIRTUAL FRONTIER: SECURITY RISKS AND VULNERABILITIES

As 3D-animated digital twins become increasingly integrated into the metaverse, they face multiple security challenges that can compromise both personal and organizational safety. These twins often contain sensitive data, including personal identifiers, behavioral patterns, and real-time activity logs, making them prime targets for cyberattacks [9]. Unauthorized access to digital twins can lead to identity theft, impersonation, or manipulation of virtual representations. Such incidents not only threaten individuals' privacy but also damage social trust and institutional credibility. One major concern is identity compromise. Because digital twins closely mirror real people, attackers can exploit them for fraudulent activities, social engineering, or reputation damage [20]. Virtual impersonation in the metaverse can be difficult to detect because of the immersive and interactive nature of 3D twins, which increases the risk of deception. Similarly, data breaches can expose private information, including biometrics, personal preferences, and location data, raising legal and ethical concerns regarding consent and accountability [21]. Another challenge is the unauthorized manipulation of the data. Hackers or malicious users can modify the behavior or appearance of digital twins to mislead others, simulate false interactions, or disrupt collaborative environments [22]. Such manipulation can undermine professional simulations, educational exercises, or healthcare modelling, producing real-world consequences.

Additionally, the interconnectedness of digital twins within the metaverse amplifies their vulnerability. A compromised twin can affect the linked systems, causing cascading effects across networks and platforms. Security concerns are compounded by insufficient governance and regulations. Current frameworks often lag behind technological advances, leaving users and organizations exposed [19]. The dynamic nature of the metaverse, where digital twins are constantly updated and modified, creates challenges in monitoring access, authenticating users, and enforcing security. To mitigate these risks, stakeholders must implement a combination of technical, policy, and awareness-based strategies. Although technical solutions such as encryption, authentication protocols, and monitoring are essential, they must be complemented by ethical policies, user education, and governance frameworks to ensure the responsible and secure use of digital twins in immersive environments [20]. Proactively addressing security challenges is critical for preserving the integrity of digital twins and maintaining trust in the metaverse. Failure to do so could undermine both the potential benefits and societal acceptance of immersive digital technology.

MORAL CONSIDERATIONS FOR DIGITAL TWINS

The increasing realism of 3D-animated digital twins in the metaverse introduces several ethical risks that extend beyond technical concerns of the technology. One primary issue is consent. Individuals may not fully understand how their digital twin is created, used, or shared, raising questions about informed consent and personal autonomy [9]. Digital twins that replicate behaviors, appearances, or personal data without clear consent can violate privacy and trust. Ownership is another critical issue. When digital twins mirror individuals, it is often unclear who legally or ethically controls them. Users, developers, and platforms may all claim partial rights, creating conflicts over access, modification, and usage [23]. The mismanagement of ownership rights can result in misuse, unauthorized replication, or monetization of digital representations without the individual's knowledge.

The ethical implications of identity and representation are significant. Digital twins can exaggerate, distort, or misrepresent aspects of a person's identity, potentially leading to psychological harm or social misperception [24]. For example, manipulated twins could be used to spread misinformation or harass individuals, undermining trust in virtual communities. Similarly, digital inequality arises when access to advanced twin technologies is limited by socioeconomic status, geography, or digital literacy, exacerbating existing societal disparities [25]. Accountability is another concern. When actions are performed by or through a digital twin, determining responsibility for errors, harm, or misconduct becomes complicated. The misuse of digital twins in educational, healthcare, or professional contexts can have real-world consequences, but existing frameworks rarely provide clear guidance [26].

To address these ethical challenges, developers and policymakers must adopt transparent, fair, and socially responsible principles. Users should be informed about the data collection, use, and representation of their digital twins. Guidelines for ownership, modification, and access must be established to protect individual rights. Additionally, ethical awareness programs and digital literacy initiatives can empower users to navigate virtual environments safely and responsibly [9]. Ultimately, the ethical management of 3D-animated digital twins is critical for fostering trust, inclusion, and fairness in the metaverse. Without clear ethical frameworks, the adoption of these technologies could harm individuals and communities, limiting the social benefits of immersive virtual experiences.

For policymakers, it also surfaces societal challenges such as unequal access to technology, potential misuse of surveillance data, and the digital divide between communities [17]. Finally, in the gaming and social metaverse, platforms such as Decentraland and Roblox allow users to create avatars or digital twins that represent themselves. Reports of identity impersonation, harassment, and exploitation highlight the ethical and social risks of interactive digital twins, stressing the need for policies that ensure privacy, consent, and protection against misuse [29]. These case studies demonstrate that while digital twins offer substantial benefits across industries, careful consideration of security, ethics, and societal impacts is essential. They underscore the need for integrated strategies that balance innovation with responsible management to ensure that digital twins enhance, rather than compromise, human experiences.

CONCLUSION

3D-animated digital twins in the metaverse offer unprecedented opportunities for interaction, learning, and simulation. They bridge the physical and digital worlds, enabling immersive experiences in education, healthcare, business, and social environments. These tools allow users to explore complex scenarios safely, collaborate remotely, and gain insights that were previously difficult or impossible to achieve in the real world. However, the adoption of digital twins introduces significant security, ethical, and societal challenges. Security risks, such as identity theft, data breaches, and unauthorized manipulation, can compromise personal safety and trust. Ethical concerns regarding consent, ownership, representation, and accountability require careful consideration to protect individuals and communities. Societal implications, including psychological effects, digital inequality, and altered social norms, highlight the broader consequences of the unchecked use of these technologies. Addressing these challenges requires integrated strategies that combine technical safeguards, ethical governance, user education, interdisciplinary collaboration, and regulatory frameworks. Data protection, transparency, and responsible management of digital twins are essential for maintaining trust and fostering equitable access to technology.

Ethical policies and digital literacy initiatives help users understand the implications of their virtual representations, and interdisciplinary collaboration ensures that solutions are socially responsible and contextually relevant. Ultimately, the potential of 3D-animated digital twins can only be realized when innovation is paired with responsibility. By proactively considering security, ethics, and societal impacts, developers, policymakers, and users can create a metaverse that is safe, inclusive, trustworthy, and user-friendly. The responsible integration of digital twins has the potential to enhance human experience, support informed decision-making, and contribute positively to society. However, without

careful oversight and ethical awareness, these technologies may exacerbate risks, inequality, and harm. This study underscores the importance of balancing technological advancement with ethical responsibility. Only through such a balance can digital twins in the metaverse deliver meaningful benefits while minimizing potential threats to individuals and society at large.

REFERENCES

1. Rosen R, Von Wichert G, Lo G, Bettenhausen KD. About the importance of autonomy and digital twins for the future of manufacturing. *IFAC-PapersOnLine*. 2015;48:567-72. doi:10.1016/j.ifacol.2015.06.141.
2. Liao SM, editor. *Ethics of Artificial Intelligence*. Oxford: Oxford University Press; 2020.
3. Calo R. Artificial intelligence policy: a primer and road map. *Univ Bologna Law Rev*. 2018;3:180-218.
4. Calo R. Robotics and the lessons of cyberlaw. *Calif Law Rev*. 2015:513-63.
5. Bowen GA. Document analysis as a qualitative research method. *Qual Res J*. 2009;9:27-40. doi:10.3316/QRJ0902027.
6. Rossi de Borba JG, Dias Canedo E. Bridging theory and practice: ethical AI user story generator (EAI-USG)—a tool for translating ethical AI requirements into ethical user stories. SSRN [Preprint]. Available from: SSRN 5312104.
7. Alcaraz C, Lopez J. Digital twin: a comprehensive survey of security threats. *IEEE Commun Surv Tutor*. 2022;24:1475-503. doi:10.1109/COMST.2022.3171465.
8. Bhattacharyya DK. *Organizational Structure and Design: Text and Cases*. Routledge India; 2024.
9. Putnam RD. *Bowling Alone: The Collapse and Revival of American Community*. New York (NY): Simon & Schuster; 2000.
10. Yee N, Bailenson JN. The difference between being and seeing: the relative contribution of self-perception and priming to behavioral changes via digital self-representation. *Media Psychol*. 2009;12:195-209. doi:10.1080/15213260902849943.
11. Kritzinger W, Karner M, Traar G, Henjes J, Sihn W. Digital Twin in manufacturing: a categorical literature review and classification. *IFAC-PapersOnLine*. 2018;51:1016-22. doi:10.1016/j.ifacol.2018.08.474.
12. Creswell JW, Poth CN. *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Thousand Oaks (CA): SAGE Publications; 2016.
13. Tao F, Zhang M, Nee AY. *Digital Twin Driven Smart Manufacturing*. London: Academic Press; 2019.
14. Wajcman J. Addressing technological change: the challenge to social theory. *Curr Sociol*. 2002;50:347-63. doi:10.1177/0011392102050003004.
15. Braun V, Clarke V. Using thematic analysis in psychology. *Qual Res Psychol*. 2006;3:77-101. doi:10.1191/1478088706qp063oa.
16. Negri E, Fumagalli L, Macchi M. A review of the roles of digital twin in CPS-based production systems. *Procedia Manuf*. 2017;11:939-48. doi:10.1016/j.promfg.2017.07.198.
17. Jones D, Snider C, Nassehi A, Yon J, Hicks B. Characterising the Digital Twin: a systematic literature review. *CIRP J Manuf Sci Technol*. 2020;29:36-52. doi:10.1016/j.cirpj.2020.02.002.
18. Umbrello S, Van de Poel I. Mapping value sensitive design onto AI for social good principles. *AI Ethics*. 2021;1:283-96. doi:10.1007/s43681-021-00038-3. PMID:34790942.
19. Shehab MJ, Kassem I, Kutty AA, Kucukvar M, Onat N, Khattab T. 5G networks towards smart and sustainable cities: a review of recent developments, applications and future perspectives. *IEEE Access*. 2022;10:2987-3006. doi:10.1109/ACCESS.2021.3139436.
20. Uhlemann THJ, Lehmann C, Steinhilper R. The digital twin: realizing the cyber-physical production system for industry 4.0. *Procedia CIRP*. 2017;61:335-40. doi:10.1016/j.procir.2016.11.152.
21. Schroeder R. *Social Theory After the Internet: Media, Technology, and Globalization*. London: UCL Press; 2018.
22. Bailenson J. *Experience on Demand: What Virtual Reality Is, How It Works, and What It Can Do*. New York (NY): W. W. Norton & Company; 2018.

23. Floridi L. *The Logic of Information: A Theory of Philosophy as Conceptual Design*. Oxford: Oxford University Press; 2019. doi:10.1093/oso/9780198833635.001.0001.
24. Floridi L. Faultless responsibility: on the nature and allocation of moral responsibility for distributed moral actions. *Philos Trans A Math Phys Eng Sci*. 2016;374:20160112. doi:10.1098/rsta.2016.0112. PMID:28336791.
25. Lee J, Bagheri B, Kao HA. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manuf Lett*. 2015;3:18-23. doi:10.1016/j.mfglet.2014.12.001.
26. Fraga-Lamas P, Fernández-Caramés TM. A review on blockchain technologies for an advanced and cyber-resilient automotive industry. *IEEE Access*. 2019;7:17578-98. doi:10.1109/ACCESS.2019.2895302.
27. Lin JM, Latoschik ME. Digital body, identity and privacy in social virtual reality: a systematic review. *Front Virtual Real*. 2022;3:974652. doi:10.3389/frvir.2022.974652.
28. Jobin A, Ienca M, Vayena E. The global landscape of AI ethics guidelines. *Nat Mach Intell*. 2019;1:389-99. doi:10.1038/s42256-019-0088-2.
29. Gunkel DJ. *The Machine Question: Critical Perspectives on AI, Robots, and Ethics*. Cambridge (MA): The MIT Press; 2012. doi:10.7551/mitpress/8975.001.0001.
30. Fuller A, Fan Z, Day C, Barlow C. Digital twin: enabling technologies, challenges and open research. *IEEE Access*. 2020;8:108952-71. doi:10.1109/ACCESS.2020.2998358.
31. Bruynseels K, Santoni de Sio F, Van den Hoven J. Digital twins in health care: ethical implications of an emerging engineering paradigm. *Front Genet*. 2018;9:31. doi:10.3389/fgene.2018.00031. PMID:29487613.
32. Glaessgen E, Stargel D. The digital twin paradigm for future NASA and US Air Force vehicles. In: *Proceedings of the 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference; 20th AIAA/ASME/AHS Adaptive Structures Conference; 14th AIAA*. 2012. p.1818.
33. West SM. Data capitalism: redefining the logics of surveillance and privacy. *Bus Soc*. 2019;58:20-41. doi:10.1177/0007650317718185.
34. Sundaravadivazhagan B, S B, Raj P, Kumari KS, editors. *Applying Metaverse Technologies to Human–Computer Interaction for Healthcare*. Boca Raton (FL): Auerbach Publications; 2025. doi:10.1201/9781003491668.
35. Kshetri N. Blockchain's roles in meeting key supply chain management objectives. *Int J Inf Manage*. 2018;39:80-89. doi:10.1016/j.ijinfomgt.2017.12.005.
36. Grieves M, Hua EY, editors. *Digital Twins, Simulation, and the Metaverse*. Cham: Springer Nature Switzerland; 2024. doi:10.1007/978-3-031-69107-2.