Metaverse & Virtual Transformation. 2025, 1(2): 95-106.

The International Journal of Metaverse & Virtual Transformation (IJMVT)

https://mvt.artahub.ir

ORIGINAL RESEARCH ARTICLE

From Data to Digital Presence: Foundations of Digital Identity in the Metaverse

Samaneh Rahimian

[1] *PhD candidate in Information and Knowledge Management Department, Faculty of Management and Economics, University of Tarbiat Modares, Tehran, Iran. s_rahimian@modares.ac.ir, 0000-0002-9160-9609.*

ARTICLE INFO

Article History:
Received: 2025-02-12
Revised: 2025-04-24
Accepted: 2025-05-17
Published Online: 2025-06-01

Keywords:
Digital identity, Metaverse, DIKW, Systematic review, Digital presence

Number of Reference: 22
Number of Figures: 5
Number of Tables: 9

DOI:

ABSTRACT

Digital identity, as one of the fundamental pillars of user presence in the metaverse, requires a deep understanding of the process of transforming data into information and then applying knowledge. In such a context, digital identity is the cornerstone of interactions, trust, and user experience. The process of digital identity formation in the metaverse can be explained within the framework of the Data–Information–Knowledge (DIKW) hierarchy. This framework explains how raw data—including user behavior, interactions, and biological signals—are processed and contextualized into information and then knowledge, ultimately leading to the formation of a "digital presence" Using a systematic review based on the PRISMA 2020 framework, this study analyzed 42 relevant articles to clarify the path of digital identity formation in metaverse environments. The findings show that most research has focused on data collection and user information processing, while user knowledge analysis and informed decision-making have received less attention. This trend indicates a research gap at the level of digital presence management and knowledge application. By synthesizing the findings, the present study highlights the DIKW conceptual framework for digital identity in the metaverse and provides suggestions for future research, including focusing on user knowledge analysis, social and psychological aspects, international studies, and developing practical frameworks for safe and meaningful presence in the metaverse. **©authors**

►**Citation:** Rahimian, S. (2025). From Data to Digital Presence: Foundations of Digital Identity in the Metaverse. *The International Journal of Metaverse & Virtual Transformation (IJMVT)*, 1(2): 95-106.

Introduction

The rapid growth of immersive technologies such as virtual reality, augmented reality, and extended reality has paved the way for the emergence of the metaverse; a digital, sustainable, and interactive environment in which users engage in social, economic, and cultural activities through avatar (Mystakidis, 2022). In such a context, digital identity is the cornerstone of interactions, trust, and user experience. The process of digital identity formation in the metaverse can be explained within the framework of the Data–Information–Knowledge (DIKW) hierarchy. This framework explains how raw data—including user behavior, interactions, and biological signals—are processed and contextualized into information and then knowledge, ultimately leading to the formation of a "digital presence" (Frické, 2009). Unlike traditional profiles, digital presence in the metaverse is dynamic and tangible, and can persist across platforms (Dwivedi et al., 2022). Despite the growing attention to identity in the metaverse, many studies have examined the core elements of this process—data management, knowledge construction, and digital visualization—in isolation (Kye et al., 2021; Lee et al., 2021). This discrete approach ignores the interdependencies of these stages and their role in trust, privacy, and user experience.

In 2025, the metaverse has become a platform powered by real-world data. sensors and IoT devices transmit real-time physical data to virtual environments. Artificial intelligence (AI) processes and analyzes this data to deliver a more immersive mixed reality experience. AI is responsible for creating, managing, and analyzing content, including the production of images, sounds, 3D models, and non-playable characters (NPCs). AI also ensures data security and user privacy with behavioral analysis algorithms (Artificial Intelligence in the Metaverse: Its Role and Applications, 2025).

Data collection and organization that is essential to the consumer in the metaverse requires a large investment of time and effort. organizations will be able to conduct data analytics through the metaverse by disseminating information across applications. (Huynh-The,2023) and AI algorithms analyze economic and behavioral market trends in cyberspace. Knowledge in the metaverse is delivered through hands-on training, virtual and augmented reality simulations, and AI-powered decision support systems. AI can be implemented in many knowledge areas that can be personalized to facilitate individual learning styles, creativity, and learning speed and provide feedback in a learning process that prioritizes problem-solving (Ivanova & Petrova, 2023). The combination of human and intelligent decision-making blurs the line between creator and tool and transforms the process of knowledge production. There are significant challenges in data management, including maintaining security and privacy, preventing discrimination in AI algorithms, and complying with data and AI regulations. By 2025, various countries have passed strict laws to control AI and data, which will affect the operation of metaverse platforms (Artificial Intelligence in the Metaverse, 2025). This study shows that data and knowledge are not only the technical infrastructure but also the foundation that shapes metaverse experiences and applications, and that proper management of this data is key to the future success of this technology(Metaverse in 2025, 2025). The Data–Information–Knowledge–Wisdom (DIKW) framework explains the evolution of meaning from raw data to value-based decision-making. Data are raw, uninterpreted elements; information is the result of processing and contextualizing data; knowledge is formed by combining information and experience; and wisdom refers to the ethical and judgmental use of knowledge to solve

complex problems (Ackoff, 1989; Rowley, 2007). In the metaverse, this cycle is the basis for the formation of dynamic digital identities: raw data (such as avatar gestures, speech interactions, or biometric signs) is transformed into behavioral information; This information is transformed into knowledge about an individual's characteristics and preferences through long-term analysis and social contexts, and ultimately, by applying ethical and security considerations, leads to the creation of a stable and trustworthy identity in metaverse ecosystems (Dwivedi et al., 2022; Lee et al., 2021). Accordingly, this article, with a review approach, examines and analyzes the scientific literature related to the process of transition from data to wisdom and its role in the formation and sustainability of digital identity in the metaverse. In this review, an attempt has been made to categorize previous studies based on the components of the DIKW framework, identify existing research gaps, and suggest future directions for the development of conceptual and applied models of digital identity in metaverse ecosystems.

Literature Review

The Data-Information-Knowledge-Wisdom (DIKW) hierarchical framework is one of the most well-known models in information science and knowledge management that explains the evolution of the meaning and application of knowledge from raw data to value-based decision-making (Rowley, 2007). In the context of digital technologies and the metaverse, the DIKW framework allows for the analysis of the path of transforming raw data—such as user interactions, avatar movements, and biometric data—into behavioral knowledge and ultimately into a sustainable digital identity (Dwivedi et al., 2022). This model not only provides a conceptual framework for understanding the flow of data to intelligence but also a valuable tool for designing secure, interoperable, and user-centric digital identity systems in metaverse environments.

On the other hand, many daily activities take place on the Internet and in cyberspace. These factors have led to an impact and even a change in identity, and in an era where everything is becoming electronic and digital, identity has also emerged with a new dimension and nature called digital identity. According to the definition of the ISO / IEC 247601 standard, digital identity is a set of characteristics associated with an entity. The information contained in a digital identity is used to evaluate and authenticate users in connection with computer systems in the network environment (web). Using digital identity, individuals can create value and gain benefits while interacting with companies, governments, and other individuals in the roles of consumers, workers, microenterprises, taxpayers and beneficiaries, owners, and other roles; developed countries have reached an acceptable consensus on it, and every day the quality, security, and actual facilities associated with it are added to (International Bank for Reconstruction and Development, 2018).

Currently, due to the display capabilities, individuals on digital platforms can present their identity in the form of a digital identity. On the digital platform, even individuals can continuously reconstruct their digital identity. Various definitions of digital identity have been mentioned in different sources. Familiarity with these definitions leads to a better understanding of this field:

- ✓ Digital identity can be defined as the digital representation of known information about a specific individual or organization (Bertino, Lafayette, and Paci 2009).

- ✓ Digital identity is the sum of all available digital information about an entity. (Rose, Rehse, and Rober, 2012)
- ✓ Digital identity includes what you post, and even what others post about you, such as mentioning you in an article and bug, a post about you, a photo of you, registering a tag about you, or responding to a post of yours (Mansouri and Mrabet, 2013)
- ✓ Digital identity includes everything that happens via a computer connected to the network (all technical traces), including URLs, searches made, sites visited, cookies, etc. (Mansouri and Mrabet, 2013).
- ✓ Digital identity is a fundamental set of enabling technologies that can play a fundamental role in a wide range of interactions between individuals and institutions (White et al., 2019).

Also, in a more complete definition, at the 2018 World Economic Forum Annual Meeting in Davos[1] , a group of stakeholders, practitioners, governments, businesses, and civil society came together to agree on digital identity and its factors and parameters. Accordingly, five key elements for a good digital identity were introduced at the forum:

1. Fit for purpose. A good digital identity is a reliable way for individuals to be trusted with the identity they claim, to exercise their freedoms and rights, or to participate in digital interactions and transactions.
2. Inclusive. A comprehensive and inclusive digital identity allows everyone to activate, establish, and benefit from their digital identity, without the risk of discrimination based on identity data, without facing processes that might remove them.
3. Utility. A useful digital identity enables individuals to access useful transactions and services while being simple and easy to establish and use.
4. Providing choice. Individuals have the right to choose if they can identify the systems that use their identity data and understand their purposes. Being able to decide for themselves which data is made available to which systems, for what purpose, and for how long. In the absence of this right to choose, individuals are exposed to an incalculable risk of data breaches, privacy breaches, identity theft, fraud, or other abuses.
5. Secure. Security involves protecting individuals, organizations, devices, and infrastructure from identity theft, unauthorized and untrusted data sharing, and human rights violations. Such security is currently not truly and comprehensively implemented, as digital identity data has not yet been collected in a usable and citationable form, and the information is heterogeneously dispersed throughout the digital realm (Halloran, 2018). The DIKW model has a special interpretation in new technological contexts such as the metaverse. In the metaverse, users' digital identity is not simply a "virtual profile," but a dynamic and layered structure that starts from raw data and extends to deeper layers of knowledge and wisdom.

This evolution can be explained with the DIKW model:

1. Data: At the first level, digital identity relies on raw data, including biological data (such as images, sounds, body movements in a virtual reality environment), behavioral data (clicks, purchases, interactions), and social data (communication networks, groups, and digital communities). At this level, identity still lacks meaning and is just a collection of data points (Rowley, 2007).

[1] https://www3.weforum.org/docs/WEF_Annual_Report_18-19.pdf

2. Information: When this data is organized into specific formats, it becomes information (Frické, 2009). For example, metaverse algorithms identify user behavior patterns and build an "identity profile" from them. In this way, the user becomes not just an anonymous entity, but an identifiable individual with characteristics, preferences, and interests (Frické, 2009).
3. Knowledge: After passing the information stage, the user's continuous interaction with the metaverse environment and other users leads to the formation of knowledge. At this level, the digital identity moves from a passive state to actively participating in social interactions, learning, content creation, and even self-recreation. The resulting knowledge is a reflection of the user's internalization of information. In the real world, identity encompasses diverse facets such as race, age, occupation, culture, hobbies, gender identity, and sexual orientation, which are crucial for self-presence, self-expression, and pride. Yet, these same attributes can also expose individuals to risks such as bullying, harassment, stalking, discrimination, litigation, legal actions, persecution, deception, or bias (WEF, 2024). Identity in the metaverse inherits this duality from the real world, yet it becomes even more complex. The metaverse provides users with a creative space unrestricted by physical rules, allowing them to interact with other individuals and environments across various dimensions (Lee et al., 2021; Wider et al., 2023)
4. Wisdom: At the highest level, digital identity in the metaverse can become a tool for exercising wisdom and making informed decisions. This layer is realized when the user not only applies their knowledge in the digital environment, but also uses it to guide ethical actions, social responsibility, and creative participation. Wisdom here means the ability to create meaning and lasting value in the metaverse (Rowley, 2007).

Therefore, from the perspective of information and knowledge, identity-based layers can be examined. On this basis, it can be acknowledged that identity is equal to the information that is used in the introduction layer. In the subsequent layers, information is not enough, and knowledge must be used. Ultimately, the root of all of them is in data. For example, databases, systems, and various transactions were created based on data. Using this data, we access information and ultimately reach the desired knowledge. As a result, data together form information, which makes the understanding of identity more accurate. This link shows that digital identity in the metaverse is not a one-dimensional phenomenon; rather, it is on a path of transformation from data to knowledge. Based on this, some of the Applications and Implications of the metaverse are:

- Education: The metaverse offers transformative potential in education by providing immersive and engaging learning environments, improving knowledge retention and student engagement (Bala et al.2024; Villegas-Ch et al., 2024)
- Healthcare: The integration of metaverse technologies in healthcare, termed "MEDverse," can enhance patient outcomes, access to care, and professional collaboration (Rajendran& Dhanasekaran,2025)
- Business and Commerce: The metaverse promotes innovation in business models, enabling virtual-physical alliances and enhancing customer experiences through knowledge management strategies (Xin et al.,2025).

If this path is managed properly, the metaverse can be a platform for fostering personality development, promoting collective health, meaningful social identity, and developing users' cultural capital. Conversely, if identity stops at the data or information level, the likelihood of identity crisis, superficiality, and even data abuse increases (Floridi, 2014). To better

understand the connection between the DIKW framework and digital identity in the metaverse, some key studies that have examined this relationship are summarized in the table below:

Table1.*Research conducted in the field the DIKW framework and digital identity in the metaverse*

Title	Year	Author	Findings
Big Data Meets Metaverse	2022	Sun et al.	Emphasizing the importance of transforming big data into information and knowledge to advance digital identity in the metaverse.
Security of Virtual Reality Authentication Methods in Metaverse	2022	Kürtünlüoğlu, Akdik & Karaarslan	Comparison of biometric and information-based authentication methods in the metaverse with security approaches
Self-Sovereign Identity for Trust and Interoperability in the Metaverse	2023	Ghirmai et al.	With the DIKW framework, a model is presented that explains data → secure information → trusted digital identity.
Metaverse Identity: Core Principles and Critical Challenges	2024	Yang, Xu & Hui	metaverse identity should progress from data (interactions) to information and knowledge-based identity construction.
Digital identity, privacy security, and their legal safeguards in the Metaverse	2023	Wu & Zhang	Processing 3D user data requires transformation into contextual information to form a valid and reliable digital identity.
Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds.	2024	Ruiu et al.	authors show how the DIKW flow from biometric data to secure information and its management, ultimately leading to digital identity.

The above studies confirm the importance of the integration of DIKW stages in the formation of digital identity in metaverse environments: from initial data such as avatar behaviors and biometrics (Data), to the extraction and organization of meaningful information (Information), analysis and accurate understanding of the user (Knowledge). This process is not only applicable at the theoretical level but also in technical design and policy-making. Consequently, to develop future frameworks in the field of digital identity in the metaverse, it is necessary to consider layers of DIKW in a coordinated manner.

Method

This study is a systematic review based on the PRISMA 2020 guidelines (Page et al., 2020) that aims to identify and analyze the relationship between the data-information-knowledge-wisdom (DIKW) framework and digital identity in the context of the metaverse. A Scopus search was conducted with keywords such as “data”, “information”, “knowledge”, “digital identity” and “metaverse” and the time period 2007 to 2025. In this study, the data-information-knowledge-wisdom (DIKW) framework was used to analyze digital identity in the metaverse. However, the micro level was not included in the final analysis because it requires value judgments and knowledge-based practical decisions, which are not possible to extract from systematic review articles due to the limited data available. Most of the reviewed studies provide patterns of data, information and knowledge, but no specific quantitative or qualitative criteria were found to assess micro in the metaverse environment. Therefore, the research focused on the data, information, and knowledge levels to conduct structural analysis and categorize findings in a scientific and valid manner, while the micro level is beyond the scope of this study and the type of data available. Inclusion criteria included peer-reviewed, English-language, full-text, and relevant articles, and duplicate or non-scientific works were excluded. After filtering with EndNote software, title and abstract screening was performed by the researcher, and eligible items were reviewed at the full-text stage. Data were coded and main themes were extracted using qualitative content analysis. In total, out of the initial 78 articles, after screening and evaluation, 55 eligible articles were included in the final analysis. A systematic review of most of these articles showed that we

reached theoretical saturation after analyzing 42 articles. Figure 1 is a flowchart showing how to search, screen, and select articles. Figure 1 is a flowchart showing how to search, screen, and select articles.

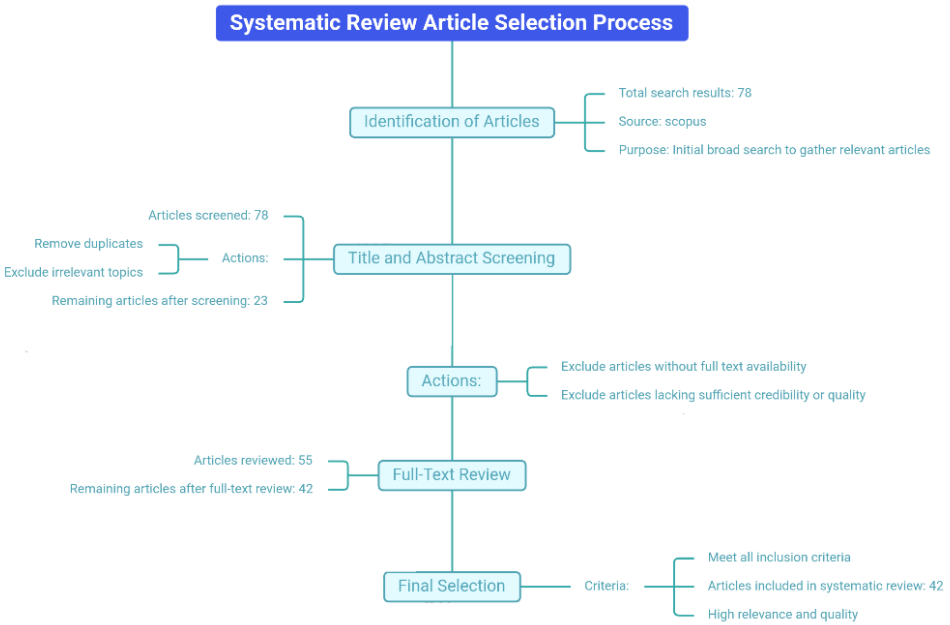

Figure 1 *.Flowchart of article search, screening, and selection*

Figure 1. Shows the flow of PRISMA 2020 in the systematic study selection process. The figure shows the number of articles identified, screened, and evaluated. The purpose of this table is to clarify how the inclusion and exclusion criteria for articles are determined.

Findings

To present the findings from the 42 reviewed articles, an analytical table was developed based on the DIKW model and digital identity in the metaverse. This table shows the number of articles related to each level of the model (data, information, knowledge) and their key findings. The purpose of this structure is to clarify the level of research coverage at each stage and identify gaps in the field of digital identity in the metaverse. In this study, a systematic review was conducted on a total of 42 articles focusing on digital identity, data, information, and knowledge in the metaverse. To provide a clear and concise overview, 10 representative articles were selected as a sample and are listed in the table below. These selected articles highlight key concepts, DIKW levels, and research trends, allowing the reader to quickly understand the scope and overall findings of the existing literature.

Table 2. *Selected sample of studies on digital identity and the metaverse with DIKW analysis*

Article No.	Author/ year	Industry/ domain	DIWK level	Data	Information	knowledge
1	Mele et al./2025	Multiple industries	Data/ Information/ knowledge	User interactions	Processed to identify patterns, technological enabler, innovation processes	Insight into how XR, AI, blockchain, NFTs enable experimentation and innovation
2	Yang et al./2025	Metaverse/digital identity	Data/ Information/ knowledge	User attributes	Framework, principles and critical challenges	Multidimensional understanding of digital selves, integration with real world identity

3	Martini/2025	Metaverse/regulation/corporate policy	Data/ information	Documents virtual worlds data	Analysis of regularly initiatives and framing of metaverse	--
4	William et al./2025	Metaverse/learning/ data protection	Data/ information/ knowledge	User behavior, empirical data	Analysis of digital identity risks, data breaches, AI ethical concerns	Understanding strategies and frameworks to protect digital identity
5	Moulika et al./2025	Metaverse/global security	Data/ information/ knowledge	Social, cultural, economic, technological data	Analysis of metaverse implications on global security privacy	Understanding risks and strategies for security, privacy, and international norms in metaverse
6	Gursoy/2025	Metaverse/cryptocurrency/cyber security	Data/information/knowledge	Price, volume data of metaverse coins	Analysis of impact of security events on coin prices and trading volume	Understanding short-term market responses and cybersecurity risks in metaverse assets
7	Matsumoto,Higo/2024	Digital identity/metaverse	Data/information/knowledge	User identity data	Descriptions of SSI infrastructure and its application to digital service	Understanding of SSI reliable identity distribution and linkage with network services
8	Al-Emran,Deveci/2024	Metaverse/cybersecurity/virtual identity	Data/ information/ knowledge	Observations of individual and organizational cybersecurity behaviors	Overview of cybersecurity measures, challenges opportunities	Understanding 0f factors influencing cybersecurity behavior and virtual identity management
9	Fiaz et al./2024	Metaverse/cybersecurity/ identity management	Data/ information/ knowledge	Technical requirements and risks of data	Analysis of limitations of centralized identity systems and need for decentralized	Proposal and validation of SSI framework for identity management in the metaverse
10	Roider,Widjaja/2024	Metaverse/privacy/digital identity	Data/ information/ knowledge	User data, industry white papers, privacy policies	Identify privacy-relevant relationships	Conceptual understanding of privacy in the metaverse from an identity perspective

The table above shows the results of 10 articles as a sample of 42 articles. The table specifies the criteria based on which each article was examined and at which level the extracted data was focused.

After reviewing and analyzing 42 selected articles in the field under study, the findings were categorized based on the DIKW (Data–Information–Knowledge) model framework. The results show that a significant portion of the articles focused on the Data–Information–Knowledge level.

For a more accurate representation, the distribution of articles based on DIKW levels is given in the table below, along with the number of articles and key findings.

Table3. *Findings DIKW, Digital Identity in the Metaverse*

Component/Axis	Number of Related Articles	Findings
Data	42	1. Basic biometric features (e.g. eye movement, voice, gait patterns) are collected as raw data that can be the basis of digital identity. 2. Avatars in the metaverse are often built from raw visual data (skin color, height, weight, clothing, tone of voice) that have not yet reached the level of interpretation. 3. Simple user transactions (login, logout, clicks, touching objects) are data collected in the metaverse to track identity. 4. Location and movement information (location in the metaverse space, speed of movement, routes) can be tracked as raw data. 5. Basic communication data (friend list, number of interactions, number of times you enter the environment) are stored, but do not have social meaning on their own. 6. Primary digital markers (username, digital wallet number, IP, blockchain ID) are data that is later processed to verify identity. 7. Content consumption details (what they watched, what they bought, what they uploaded) remain at the data level to extract behavioral patterns. 8. Physiological signals (heart rate, facial expressions, breathing if connected to a VR device) are data that is recorded in raw form.

		9. Primary preference data (choice of colors, environments, type of music or space) without analysis form part of the user's identity in the metaverse. 10. Raw digital footprints (logs and metadata related to connection time, duration of use and device used) are collected in the metaverse and form the basis for other levels of analysis
Information	42	1. User behavior patterns in the metaverse were extracted as structured information (e.g., time of presence, interaction style, type of avatar selected). 2. The classification of digital identity in the articles was presented in the form of categories such as Real Identity, Avatar Identity, and Hybrid Identity. 3. Statistical information on the level of user trust in metaverse environments shows that trust in data ownership and security directly affects the formation of digital identity. 4. Demographic information (age, gender, cultural background) in the metaverse is related to the formation of digital identity; for example, adolescents tend to have a more fluid and changeable identity. 5. The pattern of social interaction in the metaverse (friendships, groups, online communities) was extracted as key information that strengthens or weakens digital identity. 6. Security and privacy information (e.g., cyberattacks or identity theft) was reported from the articles as a serious threat to the stability of digital identity. 7. Data related to the digital economy (e.g. NFTs, virtual assets, intra-metaverse purchases) show that digital identity is linked to virtual assets and economic ownership. 8. Data from content analysis (chats, messages, avatar images) have been used as indicators to identify digital identity. 9. Comparative trends between the metaverse and social networks (e.g. Instagram or Twitter) have been recorded as comparative data, showing that identity in the metaverse is more fluid and multi-layered. 10. Ethical and social data (e.g. gender inequality or cultural discrimination in avatar selection) have been documented as data findings at the article level.
Knowledge	37	1.Digital identity in the metaverse is not just a visual profile, but also a source of socio-economic power (like a personal brand or knowledge asset). 2.Users are empowered to shape collective actions and decisions through their digital identity in the metaverse. 3.Strategic knowledge for organizations: In order to have a sustainable presence in the metaverse, companies must manage digital identity as an "intangible asset". 4.Identity continuity in time and space: The integrity and continuity of digital identity is the main challenge; users need knowledge tools to transfer identity between platforms. 5.Synergistic model between physical and digital reality: The combined knowledge of the interactions of the two spaces (phygital identity) shows that identity in the metaverse is not separate from the real world but is an extension of it. 6.Future-oriented knowledge architecture: Digital identity in the metaverse requires a dynamic knowledge framework that adapts to technological changes (such as artificial intelligence, blockchain, and the Internet of Things).
Digital Identity in the Metaverse	42	The final outcome of all DIKW levels: Trusted, Secure, and Meaningful Identity; Creating Effective Digital Interaction and Presence

Analysis of the above table shows that most of the research focused on the initial levels of the DIKW model, data and information, which highlights the importance of collecting user data and processing it for the formation of digital identity. The knowledge level, covered by 37 articles, reflects the attention to analyzing and experiencing users to manage digital presence. Overall, the findings confirm that the path of digital identity development in the metaverse continues from raw data to meaningful information, then to applied knowledge. This process both illuminates the theoretical dimensions of digital identity and helps design practical frameworks for effective and secure interactions in the metaverse.

Conclusion

In today's world, apart from personal identity and numerical and geographical addresses, another independent identity has been created for humans. Digital identity is like the footprints of humans in cyberspace and the Internet world. Email addresses, social media accounts, bank passwords and passwords set by individuals, face scans, fingerprints, eye scans and many other things are defined as the digital identity of humans in the technological era. Studies in countries around the world show that the full development of digital identity by 2030 could lead to a growth in gross national product of between 3 and 13 percent; this number varies in different countries, based on the economic problems and bottlenecks that digital identity can affect. More than half of the potential economic value created by digital identity is created for the individuals themselves, making digital identity a key to sustainable growth. Beyond measurable economic benefits, digital identity fulfills important non-

economic values; these values include political and social inclusion, protection of individuals' civil rights, and transparency. Digital identity has thus become an important paradigm in disciplines as diverse as sociology, psychology, and social studies to information science and software engineering.

A systematic review of the literature in this research revealed that the issue of digital identity in the metaverse can be explained at three levels: data, information, and knowledge. At the data level, the focus of the literature is on collecting basic user footprints, including biometrics (e.g., eye movements and voice), transactional data (login and out, clicks, movement path), physiological data (heart rate, facial expressions), and digital tokens (username, blockchain wallet, IP). These raw data do not have social meaning on their own, but they form the basis for further analysis.

At the information level, the literature has transformed raw data into interpretable patterns and categories. For example, classifying digital identity into "real identity," "avatar identity," and "hybrid identity"; extracting behavioral and social patterns; the relationship between trust, security, and identity formation; and analyzing the link between identity and the virtual economy and digital assets. At this level, data is transformed into meaningful structures, enabling comparison, measurement, and policy-making.

At the knowledge level, findings go beyond description and classification to explanation and strategy. Digital identity is not simply a visual profile, but a form of social and economic capital that can be a source of collective power and personal branding. Also, the continuity of identity over time and across platforms, the convergence of physical and digital reality in the form of "digital identity," and the need for a forward-looking knowledge architecture based on new technologies (artificial intelligence, blockchain, Internet of Things) are among the key findings at this level.

Based on the research findings, digital identity in metaverse with a multi-layered structure: data, information, knowledge can be proposed as a conceptual model in areas such as education, health, economy and social interactions. Effective management of this identity requires the integration of different stages for a secure, meaningful and sustainable digital presence of users. The main layers of this conceptual model are:

1. Data layer.
   - ✓ Components: biometric data (eye movements, voice), transactional data (entry and exit, clicks, movement path), physiological signals (heartbeat, facial expressions), digital tokens (username, wallet, IP).
   - ✓ Purpose: Collecting initial data for identity construction; a basis for subsequent analysis.
   - ✓ Applications:
     - Health: Physiological and biometric monitoring in telemedicine and virtual sports.
     - Education: Monitoring participation and learning patterns in virtual classrooms.
     - Economy: Recording transactions for virtual property ownership.
2. Information Layer
   - ✓ Components: Identity classification (real, avatar, hybrid), social and behavioral patterns, trust and security indicators, interaction with the virtual economy.
   - ✓ Purpose: Transform raw data into meaningful patterns; ability to compare, measure and make policy decisions.
   - ✓ Applications:
     - Education: Design personalized learning paths.
     - Economics: Fraud prevention and secure transactions.
     - Health: User behavior analysis for mental health and social interaction.

3.Knowledge Layer

- ✓ Components: Digital identity as social and economic capital, sustainability over time and across platforms, blending physical and digital reality, forward-looking knowledge framework using AI, blockchain and IoT.
- ✓ Purpose: Guide strategic decision-making, policy-making and informed digital presence management.
- ✓ Applications:
  - Education: Design safe and inclusive virtual learning environments.
  - Economics: Personal brand development and economic empowerment.
  - Health: Safe and ethical management of patient data in virtual services.

Accordingly, some suggestions are presented:

- ✓ For researchers:
  1. Focus on the level of knowledge and management of digital presence. Future research should pay more attention to how users analyze and use data and information to manage their digital presence.
  2. 2. Analyze psychological and social aspects. In addition to technical and data dimensions, it is essential to examine the social, psychological, and ethical implications of digital presence in future research.
  3. International and comparative studies. Examining digital identity in different metaverse environments and cultures can shed light on the global dimensions and diversity of user behaviors.

- ✓ For metaverse companies and designers:
  1. Design safe and trustworthy environments for users, with a focus on privacy and data protection.
  2. Use intelligent algorithms to transform raw data into actionable information and knowledge and provide a personalized experience.
  3. Create standards and frameworks for managing users' digital identity and the continuity of digital presence across platforms.
  4. Design educational and game-based user interfaces that enhance digital identity while increasing engagement.

- ✓ For policymakers:
  1. Develop laws and policies to protect data and digital rights of users in virtual environments.
  2. Support research and development in the field of data analysis, identity management, and the development of new technology infrastructures (AI, blockchain, IoT) in the metaverse.
  3. Investigate the social and psychological dimensions of users' digital presence and provide guidelines for reducing risks arising from digital identity.
  4. Create international and comparative platforms for the harmonization of digital identity policies and standards in metaverse environments.

References

Ackoff, R. L. (1989). From data to wisdom. *Journal of Applied Systems Analysis*, 16(1), 3–9. https://www.scirp.org/reference/ReferencesPapers?ReferenceID=713373

Artificial intelligence in the metaverse: Its role and applications. (2025). [Dataset]. In *Metatimes*. https://metatimes.ir/2025/07/16/metaverse-in-2025

Bala, M.opens author details in a new tab,Bhardwaj, B.(2024). Eco-metaverse bridge: Transitioning towards a sustainable future. *Green Transition Impacts on the Economy,*

Society, and Environment. https://www.irma-international.org/viewtitle/354204/?isxn=9798369339855

Digital Identity Protection - Concepts and Issues (2009). *International Conference on Availability, Reliability and Security, Fukuoka,* Japan. https://ieeexplore.ieee.org/document/5066445/

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., ... & Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 66, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Floridi, L. (2014). The fourth revolution: How the infosphere is reshaping human reality. *Oxford University Press.*

Frické, M. (2009). The knowledge pyramid: A critique of the DIKW hierarchy. *Journal of Information Science*, 35(2), 131–142. https://doi.org/10.1177/0165551508094050

Ghirmai, S., Mebrahtom, D., Aloqaily, M., Guizani, M., & Debbah, M. (2023). Self-Sovereign Identity for Trust and Interoperability in the Metaverse (Version 1). *arXiv*. https://doi.org/10.48550/ARXIV.2303.00422

Halloran, D. (2018). Identity in a Digital World A new chapter in the social contract. Retrieved from : https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

Huynh-The, T., Gadekallu, T. R., Wang, W., Yenduri, G., Ranaweera, P., Pham, Q. V., da Costa, D. B., & Liyanage, M. (2023). Blockchain for the metaverse: A Review. *Future Generation Computer Systems, 143,* 401-419. https://doi.org/10.1016/j.future.2023.02.008

International Bank for Reconstruction and Development. (2018). *World Development Report 2018*. World Bank. https://www.worldbank.org/en/publication/wdr2018

Ivanova, M., & Petrova, T. (2023). Towards independent students 'activities, online environment and learning performance: An investigation through synthetic data and artificial neural networks. Informatics,10(2), 37. https://doi.org/10.3390/informatics10020037

Kürtünlüoğlu, P., Akdik, B., & Karaarslan, E. (2022). Security of Virtual Reality Authentication Methods in Metaverse: An Overview (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2209.06447

Kye B, Han N, Kim E, Park Y, Jo S.(2021). Educational applications of metaverse: possibilities and limitations. 18:32. https://doi.org/10.3352/jeehp.2021.18.32

Lee, L.-H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., ... & Hui, P. (2021). All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. arXiv preprint arXiv:2110.05352. https://doi.org/10.48550/arXiv.2110.05352

Mansouri, Z., Mrabet, Y. (2013). Moroccan University Students' Online Reputation Management. *International Journal of Education and Literacy Studies*. 1 (1): 47–54. https://journals.aiac.org.au/index.php/IJELS/article/view/155

Metaverse in 2025: From failure to unprecedented opportunities in digital worlds. (2025). [Dataset]. In *Metatimes*. https://metatimes.ir/2025/07/16/metaverse-in-2025

Mystakidis, S. (2022). Metaverse. Encyclopedia, 2(1), 486–497. https://doi.org/10.3390/encyclopedia2010031

Page, M. J., McKenzie, J., Bossuyt, P., Boutron, I., Hoffmann, T., mulrow, cindy, Shamseer, L., Tetzlaff, J., Akl, E., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E., Mayo-Wilson, E., McDonald, S., … Moher, D. (2020). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. Center for Open Science. https://doi.org/10.31222/osf.io/v7gm2

Rajendran, R., S., Y. R., & Dhanasekaran, S. (2025). Metaverse Healthcare in Advancing Patient Care Through Digital Realms (pp. 203-236). https://doi.org/10.4018/979-8-3693-7245-6.ch008

Rose, J.; Olaf, R.; Björn, R. (2012). The Value of Our Digital Identity. Liberty Global Policy Series 122. Retrieved from https://www.libertyglobal.com/wp-content/uploads/2022/08/The-Value-of-Our-Digital-Identity.pdf

Rowley, J. (2007). The wisdom hierarchy: Representations of the DIKW hierarchy. *Journal of Information Science*, 33(2), 163–180. https://doi.org/10.1177/0165551506070706

Ruiu, P., Nitti, M., Pilloni, V., Cadoni, M., Grosso, E., & Fadda, M. (2024). Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds. *Multimodal Technologies and Interaction*, 8(6), 48. https://doi.org/10.3390/mti8060048

Sun, J., Gan, W., Chen, Z., Li, J., & Yu, P. S. (2022). Big Data Meets Metaverse: A Survey (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2210.16282

Villegas-Ch, W., García-Ortiz, J., & Sánchez-Viteri, S. (2024). Educational Advances in the Metaverse: Boosting Learning Through Virtual and Augmented Reality and Artificial Intelligence. IEEE Access, 12, 59093–59112. https://doi.org/10.1109/access.2024.3393776

WEF (2024). Metaverse identity: Defining the self in a blended reality. Technical report, World Economic Forum. https://www.weforum.org/publications/metaverse-identity-defining-the-self-in-a-blended-reality/

Wider, W., Jiang, L., Lin, J., Fauzi, M. A., Li, J., & Chan, C. K. (2023). Metaverse chronicles: a bibliometric analysis of its evolving landscape. *International Journal of Human–Computer Interaction*, pages 1–14. https://www.tandfonline.com/doi/full/10.1080/10447318.2023.2227825

White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., McCarthy, M. (2019). *Digital identification: A key to inclusive growth*. London: McKinsey Global Institute. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

Wu, H., & Zhang, W. (2023). Digital identity, privacy security, and their legal safeguards in the Metaverse. Security and Safety, 2, 2023011. https://doi.org/10.1051/sands/2023011

Xin, B., Song, Y., Peng, W., & Tan, H. (2025). Virtual-physical alliance in the metaverse ecosystem: Business model evolution and optimal deployment of knowledge management strategy. *Technology in Society*, 82, 102955. https://doi.org/10.1016/j.techsoc.2025.102955

Yang, L., Xu, Y., & Hui, P. (2024). Framing metaverse identity: A multidimensional framework for governing digital selves (Version 3). arXiv. https://doi.org/10.48550/ARXIV.2406.08029