International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 11
***Article Received:** 15 July 2020 **Revised:** 12 September 2020 **Accepted:** 10 October 2020*

Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds

[1] Mr. T. Thiyagarajan, [2] Dr. N. Kavitha, [3] Mrs. C. Meera Bai, [4] Dr. R. Thiyagarajan,
Department of Computer Applications, Nehru Institute of Information Technology and Management, Coimbatore, Tamilnadu, India.

Abstract: Driven by technological advances in various fields (AI, 5G, VR, IoT, etc.) together with the emergence of digital twins technologies (HDT, HAL, BIM, etc.), the Metaverse has attracted growing attention from scientific and industrial communities. This interest is due to its potential impact on people lives in different sectors such as education or medicine. Specific solutions can also increase inclusiveness of people with disabilities that are an impediment to a fulfilled life. However, security and privacy concerns remain the main obstacles to its development. Particularly, the data involved in the Metaverse can be comprehensive with enough granularity to build a highly detailed digital copy of the real world, including a Human Digital Twin of a person. Existing security countermeasures are largely ineffective and lack adaptability to the specific needs of Metaverse applications. Furthermore, the virtual worlds in a large-scale Metaverse can be highly varied in terms of hardware implementation, communication interfaces, and software, which poses huge interoperability difficulties. This paper aims to analyse the risks and opportunities associated with adopting digital replicas of humans (HDTs) within the Metaverse and the challenges related to managing digital identities in this context. By examining the current technological landscape, we identify several open technological challenges that currently limit the adoption of HDTs and the Metaverse. Additionally, this paper explores a range of promising technologies and methodologies to assess their suitability within the Metaverse context. Finally, two example scenarios are presented in the Medical and Education fields.

Keywords: *Metaverse; Human Digital Twin; privacy; digital identity; wearable*

1. Introduction

The increasing impact of digital technologies on various dimensions of societal well-being has become evident. For instance, digital technologies have the capacity to overcome geographical distances and physical obstacles, thereby facilitating networks creation and communication. An illustrative example is the utilization of digital technology to address social well-being concerns, particularly in mitigating social isolation among older adults [1]. Moreover, digital technologies have the potential to diminish prejudices and inequalities, fostering inclusiveness and accessibility across diverse socio-economic, racial, and ethnic backgrounds within broader society. Furthermore, they play a pivotal role in addressing structural inequalities, thereby empowering individuals across all generations [2]. Digital platforms support the democratization of information, enabling the creation and dissemi-nation of knowledge in a collaborative and open manner, leveraging social networks and crowdsourcing methodologies.

The emergence of the Metaverse (MV), driven by advancements in Artificial Intel-ligence (AI), 5G, Virtual Reality (VR), Internet of Things (IoT), and related technologies, holds great promise for enhancing these impacts on societal well-being and cultivating a more inclusive digital world (see Figure 1). Current endeavors to improve accessibility, especially for individuals with disabilities, are still incomplete. While comprehensive solutions are needed to overcome the various obstacles that hinder equal participation in virtual environments [3], pervasive security and privacy concerns stand as formidable barriers to its development [4]. Indeed, the MV presents a variety of potential security breaches and privacy infringements, ranging from the management of vast data streams to the implications of widespread user profiling practices and the potential biases inherent in AI algorithms. Notably, the comprehensive nature of data within the MV allows for the construction of highly detailed digital replicas of the physical world, including the concept of the Human Digital Twin (HDT)—a digital counterpart of an individual [5, 6].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 11
***Article Received:** 15 July 2020 **Revised:** 12 September 2020 **Accepted:** 10 October 2020*

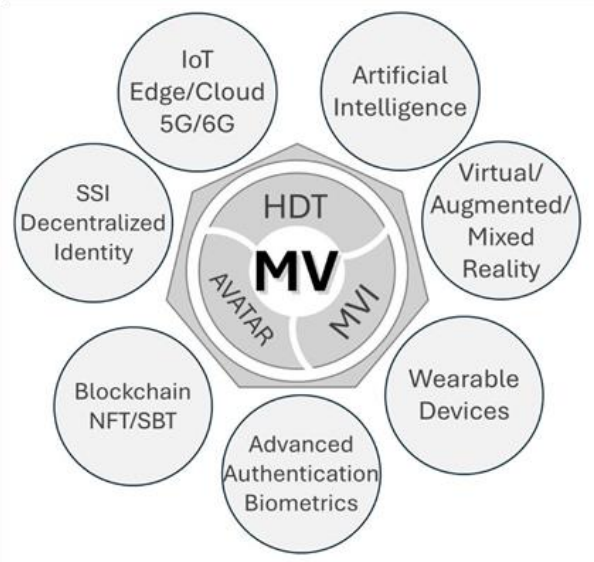

Figure 1. Key enabling technologies for the development of secure and trusted MV include the HDT and the MV Identity. These concepts are pivotal for integrating and leveraging fundamental technologies such as AI, Blockchain (BC), Non-Fungible Token (NFT) and Soulbound Token (SBT), Wearables, Self Sovereign Identity (SSI), and AR/VR environments.

The intrinsic characteristics of the MV, encompassing immersion, hyper spatio-temporality, sustainability, interoperability, scalability, and heterogeneity, present a host of challenges for effective security provision. The immersive nature of the MV, coupled with its dynamic temporal and spatial dimensions, necessitates novel security paradigms to ensure real-time monitoring and threat mitigation. Moreover, achieving sustainability in MV infrastructure poses additional complexities, requiring energy-efficient solutions and responsible resource management practices.

Interoperability emerges as a critical concern, given the diverse hardware implementa-tions, communication interfaces, and software systems inherent in virtual worlds within the MV. Since interoperability issues are caused by emerging specializations, recent research studies are focusing on comparing several types of interoperability, such as semantic, legal, or organizational, also differing in federated or unified. These also deserve investigation [7]. Solutions and tools used in other sectors, such as Building Information Modelling (BIM) in construction systems could suggest the direction in which interoperability of systems and software development together with user approach cannot be considered separately to increase efficiency [8]. The lack of standardized protocols exacerbates the challenge of seamless integration and collaboration across disparate platforms [9,10]. These challenges become even more pronounced when considering the data of vulnerable, disadvantaged, or disabled individuals, whose information and privacy are subject to heightened protection measures. Addressing the multifaceted security and privacy challenges of the MV demands a comprehensive and interdisciplinary approach. Collaborative efforts among stakehold-ers, spanning technology developers, policymakers, and researchers, are imperative to devise robust security frameworks that preserve privacy and mitigate risks while fostering innovation and accessibility within this evolving digital landscape.

This paper aims to analyze the risks and opportunities associated with the adoption of digital replicas of humans (HDT) within the Metaverse. Drawing from the current technological landscape, it identifies several open technological challenges that currently limit the adoption of HDT and the Metaverse. Fundamental questions that need to be addressed in this paper include how should humans be represented in the Metaverse? Which technologies, data, formats, and security measures will be employed? How many HDTs can an individual possess? Will digital representations be portable between worlds, or will there be one HDT per digital world? Can we trust the Metaverse, and can we exert control over our data? Are there technological solutions that can assist citizens in safeguarding their right to privacy? Additionally, the paper considers technologies that may help bridge current gaps. Furthermore, it examines usage scenarios highlighting practical adoption limitations and discusses mitigation strategies for risks.

This paper is structured as follow: Section 2 presents the scientific background and outlines key concepts. Section 3 delves into an overview of the threats and challenges posed by the integration of HDT in the Metaverse. Section 4 provides a detailed description of key enabling technologies and proposes potential solutions for mitigating security and privacy issues. Section 5 explores the implications and challenges of two socially relevant use cases, Health and Education. Finally, Section 6 draws conclusions and offers final remarks.

2. Background and Key Concepts

2.1. Digital Identity in the Metaverse

A set of attributes uniquely distinguishing a person should be collected to ascertain the identity of an individual, physically or remotely. In its most traditional form, these attributes include personal details (e.g., name, date of birth, address, social security number), while in the digital

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 11
***Article Received:** 15 July 2020 **Revised:** 12 September 2020 **Accepted:** 10 October 2020*

domain, specific information serves as a key to access particular services (e.g., username and password). A digital identity holds significant importance in the MV as it enables users to establish and uphold a consistent online persona or avatar, which can be utilized across numerous platforms and virtual environments. This identity serves as a gateway for accessing diverse services, conducting transactions, and engaging with other users within the MV. Without a trusted, interoperable digital identity, the creation of a cohesive and integrated user experience in the MV would be challenging to achieve.

The Metaverse Identity (MVI) could associated with a 3D avatar, but it encompasses more than this. Yet today, a vast amount of sensible data is streamed online from our wearable devices, including health data (e.g., heart rate, oxygen levels, and blood pressure), fitness data (e.g., number of steps taken, gps tracking, hours of sleep), along with other behavioral tracking. In particular, wearable devices can be integrated into infrastructures that provide services for patient diagnosis and management [11]. Part of these will have a role in the future model of the digital identity, since they can be used (i.e., singularly or combined) to identify a person [12,13]. Moreover, the MVI can encompass behaviors, preferences, movements, actions, and decisions made in digital spaces—whether those spaces are augmented reality (AR), virtual reality (VR), mixed reality (MR), 2D WebPages, or other platforms [14]. Even in the absence of a visual representation, our interactions and choices contribute to the formation of a distinct digital persona. This persona, although intangible, can be linked back to our real-world identities through various data points and means of identification, underscoring the intricate connection between our virtual and physical selves.

According to the World Economic Forum and Accenture [15] a Metaverse identity includes three key aspects: representation, data, and identification. An illustrative diagram of this concept is depicted in Figure 2. These fundamental aspects are inherently tied to the corresponding facets of an individual's real-life existence. For instance, in the physical world, the aspect of representation delineates how others perceive us. It is intricately linked to our outward appearance and extends to choices in dress, speech, and behavior. In the Metaverse, we have the option to retain our natural features, but it can also be more convenient to express ourselves by modifying our appearance, gender, or skin color. This expression can manifest through avatars, pseudonyms, or other digital expressions. In the real world, Identity Documents (IDs), which contain personal information and a photo, serve as the primary means for identification. Additionally, various other documents or certificates, such as driver's licenses or university degrees, can be utilized to identify a person in different contexts. In the digital worlds, a plethora of data can be employed or combined to identify a user. Collectively, these data points generated by Metaverse-supporting hardware and software (e.g., AI, wearable devices, etc.) form an intricate web of information about us. This digital footprint can effectively describe our identity within the virtual environment. When individuals with impairments or disabilities are involved, additional considerations around inclusion, diversity, and accessibility will be necessary for both the representation and data aspects.

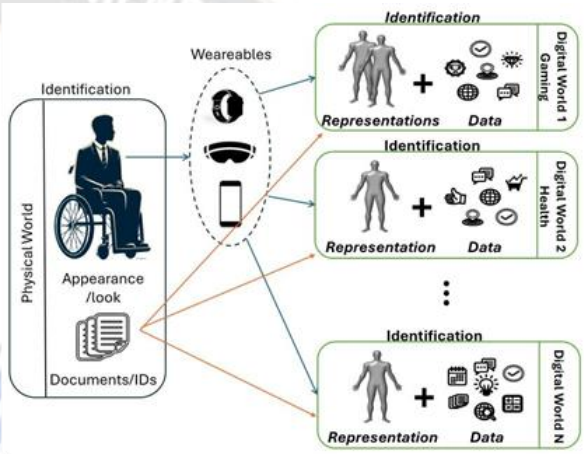

Figure 2. The main aspects of a Metaverse Identity—representation, Data, and identification—are deeply interconnected with their counterparts in the real world. These data can generate multiple MVIs across different digital worlds, each tailored to a specific theme such as health, gaming, or education. In the same digital world, a user can opt for different representations (avatars) and switch between them, similar to how it works in gaming environments.

As of today, a clear and universally recognized MVI standard has yet to emerge. Instead, there are several proprietary solutions, each employing different technologies and approaches. Among them, solutions leveraging Distributed Ledger Technology (DLT) and decentralized systems stand out as the most innovative and compelling.

2.2. Human Digital Twin

Similarly to how a Digital Twin (DT) produces a digital representation or model of a real world entity [16–18], the HDT represents a digital replica of an individual, capable of reflecting their physical, behavioral, social, physiological, psychological, cognitive, and biological

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 11
***Article Received:** 15 July 2020 **Revised:** 12 September 2020 **Accepted:** 10 October 2020*

characteristics [5,19]. Although HDTs may be analogous to DTs, there are notable differences and their design requires the integration of different types of information [20,21]. Indeed, HDTs are more complex than DTs for physical systems: they encompass the entire spectrum of human attributes, from anatomy to behavior. These dimensions interact dynamically, making an accurate modeling of HDTs challenging. For example, in [22], the author analyzes the development of a HDT from an ethical point of view, concluding that the externalization of cognitive faculties (e.g, planning, judgment, or memory) could lead to decision-making processes located within the human person to migration into digital functions. In order to develop a HDT framework, there is the need to include three distinct types of models [23]: static, dynamic, and updateable. The static models represent fixed infor-mation on an individual in the context and time frame of the scenario of use, such as a 3D form of the subject. On the other hand, the dynamic models use "historical" data to adapt and evolve over time, following specific principles, rules, or time-dependent functions. For example, an automatic learning model that uses a Deep Learning algorithm to predict an individual's actions could be trained on a set of historical data. Finally, updateable models adapt themselves considering historical inputs but also by being constantly updated with new data to improve their accuracy, spanning time and extending beyond it. For example, a personalized long short-term memory (LSTM) model can predict human decisions based on input sequences over time [24]. In [25] a unified HDT framework to integrate human factors and digital techniques to deal with complex and dynamic situations in reality is presented. This solution originates from the concept of Digital Human Modeling (DHM) which employs mathematical models and theoretical principles to simulate and predict human behavior. These models are utilized in the mechanical field, for instance, in the design of human–robot interaction. Con-versely, HDT utilizes computational resources and real-time data for continuous monitoring, prediction, and proactive interactions, emphasizing timeliness and personalized services. Additionally, these models, especially the dynamic and updateable ones, integrate data from diverse and heterogeneous sources. The HDT encompasses both static and dynamic data. Static data include personal and information, medical reports, genetic data, etc., while dynamic data include social data or that collected by wearable devices. In the Health context, the HDT can be seen as an advancement beyond the Electronic Health Record (EHR), integrating advanced visualization features that facilitate the manipulation of three-dimensional organs and body data. Figure 3 is a graphical representation which illustrates examples of data for both a male and a female individual. Usually, DTs bridge the digital and physical world through the use of a Hardware Abstraction Layer (HAL), which links the two entities: for example, a car and its DT are directly linked so that all the data produced by the car are hosted and used by the DT. In the case of the HDT, data can be obtained from a multitude of sources, which can change according to the context, so there is the need for continuous identification in order to connect the data to the rightful owner [26]. In [23], Song proposed a HDT architecture analyzing recent literature: personal data, model, and interface are the three key modules while IoT, data security, wearables, hu-man modeling, explainable AI, minimum viable sensing, and data visualization can be considered as valuable key enabling technologies. [27] surveys human digital twin models integrating various modern hardware and software components, focusing on occupational safety and health applications, also analyzing challenges and issues of existing solutions.

Figure 3. Illustrative example of HDT data that can be collected and visualized for both a male and female individual.

Finally, another difference is related to the users' avatars, i.e., to their digital repre-sentations. DTs can indeed contain the 3D representation of real-world objects so that they can be represented and interacted with in the MV. However, a user's avatar is more advanced as it receives not only the shape of the user but also all her/his related data ob-tained through the models mentioned above, thus allowing the development of a plethora of applications, such as telemedicine and personalized care or immersive learning. For example, in [28] is presented a new photogrammetric 3D modeling technique tailored to enhance the representation of virtual avatars within the digital twin paradigm, validating the solution by comparing it with avatars derived by the traditional Meshroom pipeline.

3. Threats and Challenges of the HDT Frontier

With the emergence of the MV, an increasing number of aspects of people's real lives will transition to new virtual

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 11
***Article Received:** 15 July 2020 **Revised:** 12 September 2020 **Accepted:** 10 October 2020*

worlds. Consequently, more personal and sensitive data will be transferred and stored in these virtual environments. The concern arises from the potential loss of control over this data, rendering individuals more vulnerable to cyber threats and digital disruptions caused by malicious activities in cyberspace. In this section, we will delve into various technological challenges and risks associated with data utilization in the MV. Table 1 offers a comprehensive summary of the risks delineated in this section, accompanied by their corresponding triggering factor.

Table 1. Main threats associated with the incorporation of HDT into the MV.

Threats	Causes
Identity sprawl, identity theft	Lack of standards and portability
Personal data dispersion and proliferation	Lack of interoperability, fragmentation
Lose of control of data, data lock-in or misuse	Centralization
Illegal tracking or sniffing	Wearable devices
Heterogeneity of models	Lack of standard formats and reference architectures
Difficulties in accessing HDT	Lack of user-friendly platforms
Identity theft, illegal embodiment	Difficulties in binding real person with avatars
Poor user experience	Continuous and advanced authentication which can compromise the usability of tools

One primary concern pertains to the establishment of the MV's digital identity frame-work. This prompts inquiries into the inclusion of biometric data, such as avatar appearance or vital parameters collected from wearables. Additionally, considerations arise regarding how virtual worlds can be accessed without necessitating the transfer of personal and sensitive data to third parties. To address these challenges, robust mechanisms for data management and protection within the MV must be developed. Lastly, to ensure the in-tegrity and security of HDT in the MV, reliable verification and authentication mechanisms must be established to validate the correspondence between the avatar and its real-world counterpart. This could involve the utilization of biometric recognition technologies or other advanced authentication methods. In Figure 4, a conceptualization of the exchange of data between the real world and the Metaverse is depicted, alongside some of the technological challenges involved.

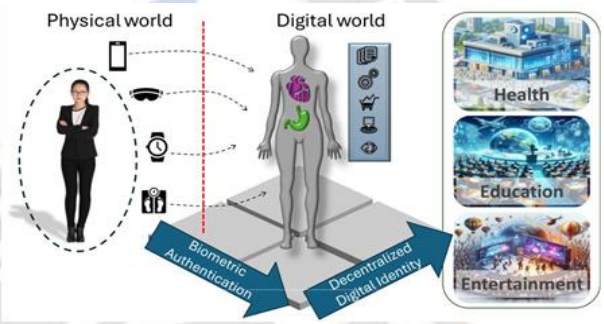

Figure 4. The boundary between the physical world and the digital one is becoming increasingly blurred. Humans contribute to the Metaverse by providing their personal data to access specialized digital environments, such as those for health, education, and entertainment. Access to the Metaverse should be secured through biometric authentication methods, while decentralized digital identity systems can ensure privacy is respected when exchanging data with service providers.

3.1. Interoperability and Centralization

One big challenge of the MV regards the lack of portability and the fragmentation of the current MVI landscape. This phenomenon is rooted in the traditional digital identity landscape, marked by a plethora of approaches and implementations that constrain data portability and service interoperability. The inability to employ the same digital identity across all services or digital worlds results in the proliferation of multiple identities linked to the same individual. This phenomenon is referred to as "identity sprawl" and entails the need to remember a large number of

credentials (password overload), which creates problems related to the usability of the solutions, forcing the user to make mistakes (e.g., using weak or repetitive passwords) that compromise the security of the systems [29]. Consequently, fraud incidents involving the fabrication of false identities or the theft of third-party digital identities are facilitated.

Furthermore, significant concerns arise when digital identity systems are structured in a centralized manner, where a third-party authority, often a private company, stores users' personal data on their servers. For these reasons, decentralized models imple-mented through blockchain technology, such as Self-Sovereign Identity (SSI), are gaining popularity [30]. Secure and privacy-preserving digital identity solutions, such as password-less authentication utilizing biometrics [31], and decentralized digital identity models like SSI, should be mandatory requirements for future digital environments [32]. Moreover, adopting interoperable and portable solutions will help prevent the proliferation and dispersion of personal data across systems managed by different entities [33].

3.2. Immersivity and Wearable Devices

Other security issues arise from the use of wearable devices, necessary to ensure immersivity and to acquire data of the user from the real world. For example, to access a virtual scene users have to wear AR/VR devices with built-in sensors. Moreover, as users need to be uniquely identified in the MV, it means that headsets, VR glasses, or other devices could be illegally used for tracking users' real locations. It has been proved that through wearable devices it is possible to gather sensitive personal information based on users' physical engagement, even without the user's consent [34,35]. Moreover, these devices enable technology to ascertain sensitive personal information based entirely on users' physical engagement with it. New forms of illegal uses of data are emerging, such as the "Biometric Psychographic", which is the gathering and use of biological data, paired with the stimuli that caused a biological reaction, to determine users' preferences, likes, and dislikes [36]. This opens up an entirely new dimension of privacy concerns, including legal questions about consent, the importance of regulation, and consumer awareness.

3.3. Expressive Representation Model

A strong heterogeneity can be observed in the use of the HDT concept across the fields where it has been applied. For example, in medicine or sports performance, the models often focus on improving human performance while in gaming or social applications, the focus is on improving the aspects of the user or the environments with which the human interacts. As a result, the components which are modeled within each of these applications differ. The digital representation can include both first principles models which are based on fundamental understanding and statistical models [37].

Moreover, since huge amounts of data subject to temporal variability (e.g., biometrics, health, behavioral, etc.) are gathered from users and stored in digital worlds, a flexible representation model for the HDT will be required. The model will be designed to sup-port dynamic instantiation, management, and deletion of its elements, and to allow easy fulfillment of the same HDT in different MV use cases.

Even if there are several efforts in the development of different models for the def-inition of HDTs to facilitate the description, prediction, or visualization of one or more characteristics of a human, there is still the need for user-friendly HDT platforms which are able to pair the real-world human twin with the corresponding HDT and provide the humans with full control of their digital counterpart.

3.4. Binding Individuals to Their Digital Twins

In the virtual and immersive realms of the Metaverse, tracing the real identities of users will become even more challenging. Identifying a user based solely on the appearance of their avatar will not be sufficient. How can we verify that the avatar is being used by the rightful owner and not by an impostor who has stolen their digital identity? Furthermore, how can we definitively ascertain the authenticity of a digital identity, distinguishing it from an AI-controlled entity?

Advanced identity verification solutions are imperative, requiring enhanced security measures and improved usability. For instance, biometric authentication can significantly mitigate the risks of identity theft and impersonation within the Metaverse by linking physical identities with digital ones. However, it should be complemented by advanced authentication modalities such as continuous methods, which verify identity continuously, ensuring consistent matching over time.

Typically, wearable devices are used to measure and transfer biometric identifiers: iris, periocular, face, and speech can be easily acquired from a VR headset, like those used for accessing the MV. However, careful consideration of biometric modality selection (e.g., single/multi, static/continuous, active/passive) is crucial depending on

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 11
***Article Received:** 15 July 2020 **Revised:** 12 September 2020 **Accepted:** 10 October 2020*

the application, as usability may be compromised otherwise. Continuous authentication is a promising approach for building a secure and trusted environment in the MV, but it still lacks in usability. Modern mobile phones largely use a mixed static and continuous paradigm. In passive authentication the user does not need to take any action. For instance, face recognition is typically designed as static–active. Gait recognition is somewhat unnatural in an active scenario, and is better performed when the user is relaxed and relatively unaware that they are being measured (continuous–passive). For an overview of Biometrics modalities and trade-offs between usability and security, see Figure 5.

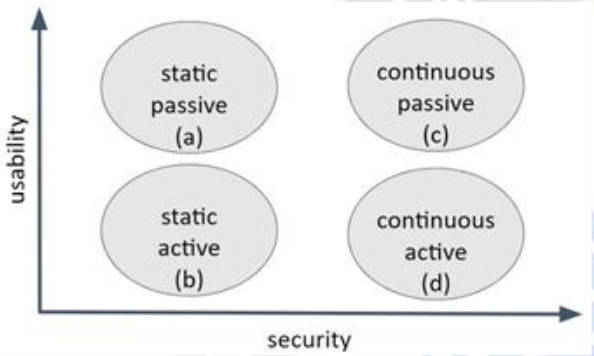

Figure 5. Graphical representation of the trade-off between security and usability in Biometric authentication systems design. Four different modalities are presented: static passive (a), static active (b), continuous passive (c), continuous active (d).

Other challenges of Biometrics authentication systems pertain to their accuracy and usability. For instance, facial recognition systems can achieve near-perfect accuracy under ideal conditions, such as clear reference images like passport photos or mugshots [38]. This enhanced accuracy is also attributed to advancements in 3D and machine learning (ML) approaches [39–41]. However, issues arise during image acquisition in unconstrained conditions, such as unclear backgrounds, facial expressions, poor lighting, and occlusions (e.g., the acquisition of facial data through an AR/VR headset).

3.5. Inclusive and Social Opportunity of the Metaverse

Based on the literature, MV is going to have a crucial societal impact [42]. The social metaverse is promoted as a paradigm oriented to face social and workplace changes drastically accelerated by the pandemic, especially for people with symptoms that make social engagement difficult [43,44].

Several challenges influence the design of solutions capable of guaranteeing inclusion, diversity, equity, accessibility, and safety [45]. Recently, several assistive technologies and innovative devices have been examined by the research community to benefit people with disabilities experiencing the metaverse [46]. Humans can be seen as the source of multi-sensory data useful to enrich the digital ecosystem. Innovative technological solutions such as Brain–Computer Interface technologies could potentially enable inclusive applications for users with disabilities in the Metaverse, such as user cognitive state monitoring, digital avatar control, virtual interactions, or imagined speech communications [47]. Models for AI disability inclusion can serve as the theoretical frameworks, guiding the development of tailored solutions [48,49]. In any case, the active involvement of physically disabled individuals in the design and development of Metaverse platforms is crucial for promoting inclusivity [50].

In the literature it is possible to find several articles that propose practical solutions to include disabled people in specific operations of daily life. In [3], the authors present a user-centric framework aiming to guide the development of an inclusive digital environment, underlining the necessity to combine technological solutions together with legal and ethical constraints in order to make metaverse inclusive. [4] provides a specific metaverse framework to allow individuals with disabilities to produce art. In [51], solutions based on assistive technologies for providing inclusive higher education for students with learning difficulties are presented. In [52], the authors presented a HDT for disabled workers capable of mapping skills and supporting the production planning and assembly processes.

4. Key Enabling Technologies

4.1. Decentralized Identity

Amidst the myriad of proposals for secure and interoperable digital identity solu-tions, decentralized identity emerges as one of the most promising and widely supported approaches. The attractiveness of a decentralized identity stems from its demonstrated capacity to reduce the quantity of data to be shared with other users and consequently the risk of exposing personal information to data brokers, data breaches, and unethical business practices [30].

A decentralized identification system is able to identify users only through interactions with other users, eliminating the necessity for a centralized registry, identity provider, or cer-tificate authority to validate them across the entire system. Nevertheless, the technologies that the

system requires, such as verifiable credentials, trusted correlation, digital wallet, digital proxy, distributed identity, blockchain technology, and governance architecture, are still immature, and a number of areas require amelioration [12].

Self-sovereign identity (SSI) represents a decentralized approach to identification, granting individuals control over their digital identities [53]. These identity systems facilitate unique, private, and secure peer-to-peer connections between parties. The fundamental technology behind SSI lies in distributed ledgers and cryptography. These components can be amalgamated with distributed digital identity identifiers and verifiable credentials to establish identity records that are non-repudiable and resistant to tampering. In this model users are the primary administrators of their identities, retaining ownership, knowledge, and discretion over its sharing.

The SSI approach adheres to the principle of data minimization, which permits the verification of specific credentials or an individual's identity without necessitating the exchange of sensitive information. This approach ensures that only the minimal necessary data is shared, thereby enhancing both privacy and security. At the core of this principle is the concept that individuals maintain full ownership and control over their personal data. This means that users have the autonomy to decide both the entities with whom they share their information and the specific manner in which these data are shared. This empowerment ensures that users can manage their privacy and security by making informed decisions about their data distribution. This principle is also crucial for complying with one of the key elements of the European data regulation (GDPR), namely, the right to be forgotten. Under this principle, data owners have the right to request the deletion of their data from service providers. Fulfilling this right with current systems is challenging, as once data are shared, owners lose control and trackability of their data. The SSI approach, through data minimization, reduces the necessity for data exchange and, when exchange is necessary, less data are shared, thereby facilitating compliance with the right to be forgotten.

SSI leverages two standards recently introduced by the World Wide Web Consortium (W3C), namely the Decentralized Identifier (DID) and the Verifiable Credential (VC). DID offers a method for individuals to create their distinct identifiers, enabling interaction within the digital world. On the other hand, a VC serves as a digital credential owned by an individual, containing pertinent information or attributes such as name, date of birth, place of residence, and more. DIDs and VCs are stored on personal devices under applications called wallets. These apps enable users to selectively disclose or minimize the information shared with other institutions. Among the most noteworthy implementations of SSI solutions are uPort [54], Sovrin [55], and Microsoft ION [56].

4.2. Non-Fungible and Soulbound Tokens

Non-fungible tokens (NFTs) enable verifiable digital ownership of distinctive items, spanning from artworks and collectibles to digital identities. The inherent attributes of NFTs, such as uniqueness, non-fungibility, transparency, and accessibility, underpin the primary rationale for advancing this concept. NFTs can be freely bought and sold to any interested party at prevailing market rates. NFT-based digital identity management entails the creation of an NFT representing the user's genuine identity, which then serves as thefocal point of identity administration within metaverses, supplanting the conventional approach [57].

NFTs currently serve as the foundation for the majority of identities within the Meta-verse. The robustness of Distributed Ledger Technology (DLT) and its decentralization ensure a high level of security and interoperability. Furthermore, by employing digital identities based on NFTs, individuals can alter their appearance by purchasing or renting different identities. This capability presents a significant opportunity for those seeking to escape their daily lives or emulate alternative lifestyles (e.g., individuals with disabilities who wish to be regarded on equal footing with others). However, it also invites criticism, from both ethical and legal points of view.

For this reason, Soulbound Tokens (SBTs) have been conceptualized [58]. SBTs are similar to NFTs, yet the primary distinction lies in their lack of commercial value and non-interchangeability, rendering them non-negotiable [59]. SBTs are publicly visible and non-transferable tokens representing commitments, credentials, and affiliations. SBTs can be attested by other Souls, who are counterparties to these relationships (e.g., individuals, companies, or institutions) [60].

Currently, numerous research groups and companies are advocating for blockchain-based identity solutions.

In [61] a mechanism for achieving Know Your Customer (KYC) processes by veri-fying user identities using smart contracts is proposed. Users acquire an SBT from the MV service provider through the DID credential issued during the KYC process. The verification of avatar identities is conducted within smart contracts, ensuring user privacy and safeguarding through Zero Knowledge Proofs (ZKPs).

Tools for generating ZKPs are provided, facilitating their convenient use even for users unfamiliar with the concept. Additionally, an integrated wallet is offered for seamless management of DID credentials and SBTs. Moreover, in instances of avatar identity disputes, users can request an audit by the issuer through associated DID tokens.

Itheum NFMe ID (https://www.itheum.io/ accessed on 2 June 2024) is the commercial solution that represents a personalized digital avatar constructed utilizing NFT technology and underpinned by an individual's authentic personal data. Users have the autonomy to mint an NFMe ID on Itheum and assert ownership over it. Moreover, additional accessories are minted and appended to the NFMe ID as more data are accumulated, each possessing unique characteristics and tradability. Pivotal to the NFMe ID are Personal Data Categories (PDCs), which are intricately linked to it. These categories serve to furnish data that are then securely stored within Personal Data Vaults. PDCs encompass various facets of personal information, encompassing financial, social, historical, gaming, and other pertinent domains. NFMe IDs are meticulously designed for interoperability, empowering users to traverse diverse Metaverses, ecosystems, and virtual realms seamlessly.

DNVerse (https://dnaverse.io/ accessed on 2 June 2024) is a decentralized platform dedicated to replicating organic life within the MV through the creation of customized art pieces utilizing real DNA data. Each member of the community contributes their DNA data, which are then integrated into art NFTs tailored to their individual uniqueness, resulting in the creation of exclusive 1 of 1 NFTs. Originally launched on the Ethereum network, the project has since transitioned to the Polygon network to optimize benefits for community members, streamline the breeding process, and enhance the ecosystem by reducing gas costs, ensuring sustainability, fostering scalability, and promoting an eco-friendly workflow on the blockchain. According to the creators, the project holds potential for multifaceted evolution. This includes applications such as authenticating humans in digital environments against artificial intelligence, personalizing digital assets to reflect one's true essence, integrating biological data and structures into digital avatars, and even exploring the possibility of transferring consciousness into the Web3 realm.

4.3. Advanced Biometric Authentication

Continuous Biometric Authentication (CA) is the process of repeatedly authenticating the biometric characteristics of a person who is engaged with a system, ensuring that at all times the person remains the same. CA must operate non-cooperatively and be non-intrusive to preserve the usability of a system. Behavioral biometrics, where the characteristic patterns of a user's activity form the index for identification, have been heavily investigated for use with mobile devices. [62–64] discuss keystroke recognition as a means for recognizing a user. Articles on gait calculated from mobile phone motion sensors [65,66], behavioral profiles derived from app usage, location or device usage frequency [36,67], touch gestures using mobile phones [65], and physiological biometric techniques [5] can be found in the literature. Similarly to gait, the motion sensors in mobile devices can also identify a user by their hand motions [38,68].

Face, periocular, and irises are useful if the user is likely to remain in a static pose, i.e., sitting at a computer, wearing a VR headset. Fingerprint or palmprint recognition can be used if the sensor is either in a regularly contacted spot, i.e., keys on a keyboard or the handle of a VR controller. Largely, CA methods use multiple biometric modalities and fuse the results to obtain greater accuracy. Fusion can be performed early where the features extracted are combined in some way before classification [69]. The alternative is late fusion where individual modalities or samples are classified and then the resultant scores, confidences, or decisions are combined to form the final decision [70].

4.4. Immersive Digital Environments

In the context of the MV, a significant consideration is the design of environments that will accommodate human replicas. A variety of metaverse platforms exist, each offering the capability to create or utilize virtual environments that span a spectrum of realism. Notable among these platforms are Decentraland, Roblox, Microsoft Mesh, and Horizon Worlds. However, an alternative approach involves creating virtual environments from scratch. This can be achieved using graphic engines such as Unity (https://unity.com/ accessed on 2 June 2024) and Unreal Engine (https://www.unrealengine.com/en-US accessed on 2 June 2024). Initially conceived for video game development, these engines have transcended their original purpose and are now gaining prominence in the realm of interactive world development.

These environments, which can meticulously recreate the world as we perceive it, serve a dual purpose. Firstly, they provide a familiar setting for visitors to the MV, fostering a sense of comfort and ease. Secondly, they harness the potential of the MV to revolutionize the field of architecture and construction. The utilization of real-world data is a cornerstone of this revolution. It enables accurate

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 11
***Article Received:** 15 July 2020 **Revised:** 12 September 2020 **Accepted:** 10 October 2020*

simulations and predictions, thereby facilitating an understanding of how to enhance the real world.

In this context, BIM plays a pivotal role [71]. BIM is a collective process that involves the creation and utilization of building information. This information forms the foundation for all decisions made during a facility's life cycle, spanning from planning and design to the release of design documents, construction, operation, and ultimately, demolition [8]. The principles of BIM can be applied at various scales—from individual buildings to neighborhoods, public spaces, and even entire cities. This application physically bridges the gap between the real world and the virtual one, underscoring the transformative potential of integrating digital and physical spaces. In the domain of urban planning and architectural design, the fusion of these two worlds through realistic virtual environments and BIM paves the way for innovation and improvement in our built environment. However, the adoption of BIM in the MV inherently encompasses the identical challenges pertaining to data security and privacy that are prevalent in various other sectors [72,73].

The application of virtual reality in the creation of immersive worlds is not without its challenges. These complexities encompass the use of headsets, the requirement for high-speed networks, and the demand for substantial computational power for the rendering of 3D environments. Headsets, a crucial component of the virtual reality experience, remain a significant investment since they are still quite expensive. Furthermore, extended usage can result in physical discomfort or social issues, manifesting as symptoms such as nausea, dizziness, and headaches [74]. Furthermore, as the volume of data transferred between the digital world and the MV, or among MV users, continues to increase, there will be a growing need for networks with broad bandwidth and minimal latency [75]. In this context, progressively efficient compression systems [76], and the convergence of edge and cloud computing [64], can offer substantial support. Lastly, the rendering of 3D environments and handling of 3D data in the MV necessitates significant computational resources. Currently, these resources are not only expensive but also pose considerable challenges for users lacking technical expertise. The future will call for increasingly powerful and compact hardware that can be integrated into portable devices, making them accessible to a broad range of users.

5. Harnessing HDT across Metaverse Worlds

The Metaverse, although not yet fully defined, represents a significant technological trend that will have substantial impacts on citizens' lives. Given the potential of combining virtual worlds and digital replicas of humans, these immersive technologies offer great potential in different sectors (e.g., education, travel, industry, and medicine), however, they also enable the collection of huge amounts of sensible data, that if not properly secured and controlled can affect the lives of future citizens.

In this section, we explore two of the most influential societal use cases of the Metaverse in the sectors of Health and Education. We underscore their potential and the benefits they offer.

5.1. Telemedicine and Personalized Care

In this section two use cases illustrating the usage of HDT and the Metaverse in the medical field are described, showcasing their potential and developments in this domain.

A medical consultation at a specialist's clinic is an experience that touches nearly everyone. Imagine having your very own digital counterpart (HDT) housed within a cutting-edge technological platform, ready to be shared with a medical professional. The HDT acts as a vast repository of information, gathering data from a variety of sources. From the constant monitoring of vital signs through wearable devices to tracking physical or athletic progress, it encapsulates a holistic view of one's health journey. Moreover, it consolidates all medical examination reports over time. Advances in gender-specific medicine, which examines how biological differences based on sex and socioeconomic and cultural differences based on gender influence health, will soon allow for a more inclusive health care, with a positive impact on prevention and treatment for women, men, and across all genders [77]. The HDT can be of great use in this scenario, by being gender-specific, from collecting gender-specific data from the patient to helping physicians to navigate through them. The HDT can therefore embed data and 3D reconstructions, both of the entire body and of specific portions, that capture the essence of the patient. According to this vision, the HDT can be seen as an evolution of the Electronic Health Record (EHR), allowing the development of digital replicas of organs and body parts that mimic their functions and shapes [78,79]. These detailed models can be explored and manipulated using cutting-edge 3D visualization, AR, VR, and MR technologies. Additionally, these tools can facilitate collaboration among specialists, allowing them to share, view, and edit data simultaneously from different locations.

This vast amount of highly sensitive data can be shared as needed by patients with various physicians to seek opinions

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 11
***Article Received:** 15 July 2020 **Revised:** 12 September 2020 **Accepted:** 10 October 2020*

or diagnoses, enabling a new form of Personalized Healthcare (PH), tailored to the individual's needs. PH (i.e., Precision Medicine) has the potential to eliminate unnecessary side effects and to reduce the high costs associated with the traditional generalist approach commonly employed in the healthcare system [80]. AI plays a central role in the implementation of PH, but it requires meticulous learning and the creation of multiple high-performance, personalized feature models customizedfor individuals, involving diagnosis, treatments, patient engagement, and adherence, or management applications [81,82]. This process hinges on the availability of extensive, high-quality training datasets for each person. Wearable devices can be employed to track and collect a continuous stream of biological data, which can be utilized for this purpose.

The ownership and control of these shared data should always remain under the patient's control. The MV will be the virtual space in which the data from the HDT can be accessed and shared. Envision virtual worlds dedicated to healthcare, where patients can access clinics, medical practices, and entire hospitals reconstructed in stunning 3D.

The benefits of such a perspective are manifold:

1. Consolidating all expertise in a centralized location, accessible remotely through AR/VR headsets, eradicates the necessity for physical travel.

2. Enhanced data sharing and visualization within immersive VR and 3D environments facilitate the manipulation and augmentation of data through the integration of diverse sources.

3. The capability to share data with disparate specialists enables multidisciplinary con-sultations and comparisons, despite physical separation.

4. Leveraging telepresence technologies enables live 3D reconstruction, generating a real-time replica of the patient within the digital environment during consultations.

The integration of these components facilitates the conceptualization of several utiliza-tion scenarios.

The first use case entails a remote virtual medical consultation at a specialist's office, albeit with the specialist located at a considerable distance from the patient geographically. Herein, the patient, situated at home, can seamlessly access the MV to schedule an appoint-ment with a doctor, selecting from those available the one they deem most suitable for their needs (see Figure 6).

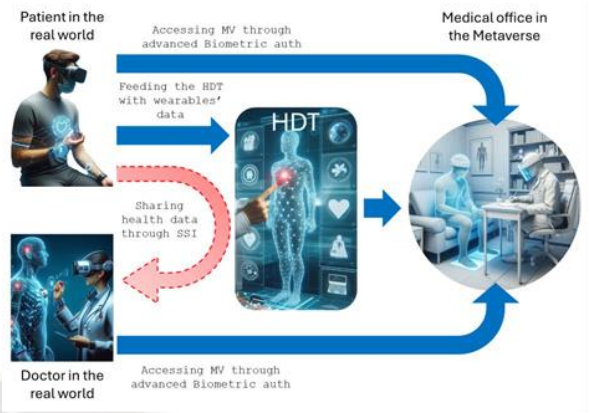

Figure 6. Schematic representation of the first use-case, a medical consultation in the Metaverse. The figure illustrates the seamless integration of virtual technologies and healthcare services in the Metaverse, offering users a convenient and personalized approach to remote medical consultations.

Initially, the patient may opt for passive engagement with the doctor, granting access to their HDT. Through the utilization of a VR headset, the doctor can review the data and formulate preliminary assessments. If necessary, the doctor could prompt the patient to en-gage via a telepresence system, enabling the real-time acquisition of additional information facilitated by the visualization of the patient's live reconstruction.The second use case involves a virtual consultation involving multiple specialist physi-cians from various geographical locations. In this instance, both doctors and the patient would convene within the same 3D environment, facilitating collaborative discussion while visualizing the same dataset (see Figure 7). This scenario proves particularly advanta-geous for cases involving rare or challenging-to-diagnose pathologies, as well as conditions affecting multiple organ systems [83–85].

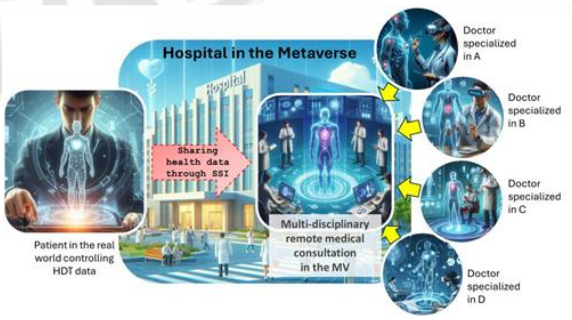

Figure 7. Schematic representation of the second use-case, a multi-disciplinary medical consultation in the Metaverse. Patients can interact with multiple doctors possessing

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 11
***Article Received:** 15 July 2020 **Revised:** 12 September 2020 **Accepted:** 10 October 2020*

various specialized skills, even when they are in remote locations, by sharing their data within the same virtual environment.

These scenarios demonstrate that, if appropriately designed, these technologies have the potential to overcome significant barriers, serving as valuable tools for social inclusion. Primarily, they enable the reduction of distances, allowing individuals to access the best expertise for their health concerns regardless of geographic location. Distance poses a substantial obstacle, particularly in regions with limited infrastructure and effective connectivity, such as remote islands or mountainous areas, where travel may be practically impossible. Moreover, for certain individuals—such as those with physical disabilities, caretakers of non-independent persons, or those facing economic challenges—distance exacerbates existing inequalities. For this reason, applications in the healthcare sector that harness the benefits of the MV and the HDT serve as effective tools for overcoming geographical and economic barriers, thereby enabling fairer and more democratic access to medical care.

5.2. Immersive Learning

The Education sector emerges as a highly promising and rapidly advancing domain within the MV, boasting a plethora of ongoing application developments. This momentum stems from the profound potential of immersive learning experiences. Furthermore, factors such as the recent global pandemic (COVID-19) and the impacts of climate change [86], underscore the imperative for innovative solutions. The greatest education disruption was seen in low- and middle-income countries, where the percentage of children who cannot read and comprehend a simple sentence rose from 57% in 2019 to 70% in 2021 [87]. AR/VR technologies can ensure uninterrupted academic operations amidst such disruptions and has the potential to boost fair and inclusive education systems. However, the adoption of emergency solutions has exposed significant shortcomings that warrant thorough analysis and rectification. The emergence of the MV presents an opportunity to reevaluate these solutions, both from a technological and legal standpoint, with the aim of creating systems that are more privacy-preserving, inclusive, and interoperable. Schools and universitierequire robust and trusted ICT solutions to ensure operational continuity, fulfill institutional mandates, and uphold students' right to education. Metaversity or MetaUniversity is a term that refers to an immersive university envi-ronment that combines VR and AR technologies, a DT of a physical campus where students and faculty can interact with each other via their digital twin avatars. Numerous universities are actively engaging in these projects, with a growing global expansion in course offerings. In 2021, Stanford University launched its first virtual reality classroom, utilizing the Meta Quest 2 platform to delve into topics spanning popular cul-ture, engineering, behavioral science, and communication. This pioneering initiative is a component of an ongoing study led by Stanford's Virtual Human Interaction Lab, which aims to explore the efficacy of virtual technologies within educational environments [88]. The University of South Wales is developing "Mediverse", a digital medical platform, created by the training company Goggleminds, which has recreated a virtual hospital where students can experiment with VR and gamification, without putting themselves or patients at risk [89]. Meta recently entered as a partner of some American universities with the Meta Immersive Learning project and is supporting ten universities to get virtual campuses off the ground with an infrastructure investment of 150 million dollars [90]. In [91], a system providing an environment to verify the credibility of students was pro-posed, based on Soulbound Tokens(SBTs). Numerous initiatives within this domain strive to develop solutions that enhance the immersive quality of the educational experience. However, there is a pressing need for a secure, privacy-preserving, and interoperable identity framework to facilitate trusted data exchange within virtual environments. For example, identification operations, including onboarding, registration, and authentication, are crucial for both students and faculty members. Effective and trusted solutions have the potential to enhance usability, save time, improve privacy by disclosing only necessary information, and enhance inclusiveness and privacy for students with disabilities, who require specialized support. Also, in this case the SSI approach seems to be a valuable option. The students create and manage their own identities by generating a unique identifier, which can be associated with personal information such as national identity cards, driving licenses, and diplomas of their educational qualifications (as depicted in Figure 8).

Figure 8. In the Metaverse, a student's Digital Identity encompasses various types of information and data, including personal details, certifications verified by third-party entities, medical certifications for special needs, credentials for accessing restricted areas, and enrollment status. Professors in the Metaverse can identify students leveraging SSI and advanced visualization tools.The digital identity of individuals will comprise a collection of personal information and certifications verified by third-party entities. Held by the individual, this compilation ensures the identity's uniqueness and reliability. A tentative architecture of the logic of a solution adopting the SSI approach has been drafted in Figure 9.

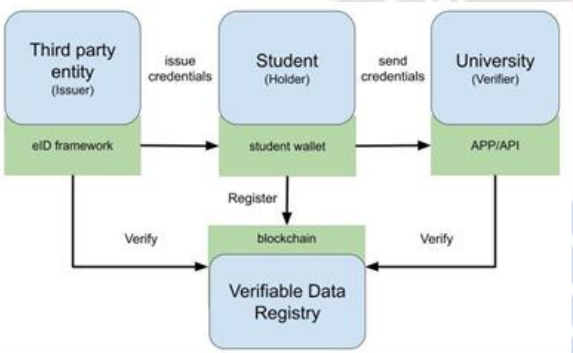

Figure 9. Flow between the entities of an SSI application (blue) and underlying infrastructures (green).

Two common scenarios could benefit from this solution:

• Lecture scenario: access to the class will be restricted solely to students officially en-rolled in the course, meaning those who can provide evidence of having successfully completed prerequisite courses and met associated requirements.

• Exam scenario: to authenticate the student's identity, it would be necessary to verify the student ID, a facial image, enrollment in the exam, and any disability certificates (e.g., to provide appropriate support if needed). The authentication process could take place at the start of the exam, with the information accessible to the professor throughout the entire duration of the exam.

The solution should aim to enhance inclusivity and privacy management for students with Specific Learning Disorders (SLD). Accessing necessary support for these students can often be a lengthy and cumbersome process, owing to confidentiality obligations that safeguard students' privacy rights. For instance, currently, verification of such sensitive information must be exclusively conducted by individuals with specific duties. A tool implementing the Self-Sovereign Identity (SSI) paradigm could empower students to directly communicate their condition during exams, sharing only pertinent information. This information could then be accessed by the professor in accordance with specific regulations that ensure privacy protection.

In the literature, there are relatively few works addressing SSI within the context of education. A recent study offers a survey of SSI in education, presenting an overview of challenges and potential solutions within the European digital credentials sector en-abled by blockchain technology. However, it is worth noting that specific implementation specifications have not yet been provided [92]. Another study presents a solution imple-mented using Alastria [93], which is notably simple but lacks significant details. These include specifics regarding user credentials, the verification process for credentials, and the involvement of issuers.

6. Conclusions

With the advent of the Metaverse, an extensive amount of data will be uploaded online to fuel the digital worlds where part of our daily lives will unfold. A significant portion of these data will be personal and sensitive, encompassing biological, behavioral, and social information. These data will shape the content and digital representations of individuals in the Metaverse, known as Human Digital Twins (HDTs). These highly representative data could be used for the digital identification of avatars, representing an advanced form of digital identity.

References

1. OECD. Educating 21st Century Children; OECD's Centre for Educational Research and Innovations: Paris, France, 2019; p. 284. [CrossRef]
2. Turk, Ž. Interoperability in construction–Mission impossible? Dev. Built Environ. **2020**, 4, 100018. [CrossRef]
11. Fuller, A.; Fan, Z.; Day, C.; Barlow, C. Digital twin: Enabling technologies, challenges and open research. IEEE Access **2020**, 8, 108952–108971. [CrossRef]
12. Barricelli, B.R.; Casiraghi, E.; Gliozzo, J.; Petrini, A.; Valtolina, S. Human digital twin for fitness management. IEEE Access **2020**, 8, 26637–26664. [CrossRef]
13. Sparrow, D.; Kruger, K.; Basson, A. Human Digital Twin for Integrating Human Workers in Industry. In Proceedings of International Conference on Competitive Manufacturing (COMA 19) Proceedings, Stellenbosch, South Africa, 30 January–1 February 2019; p. 259.

14. Dahia, G.; Jesus, L.; Pamplona Segundo, M. Continuous authentication using biometrics: An advanced review. Wiley Interdiscip. Rev. Data Min. Knowl. Discov. **2020**, 10, e1365. [CrossRef]
15. Chaudhary, S.; Schafeitel-Tähtinen, T.; Helenius, M.; Berki, E. Usability, security and trust in password managers: A quest for user-centric properties and features. Comput. Sci. Rev. **2019**, 33, 69–90. [CrossRef]
16. Bye, K.; Hosfelt, D.; Chase, S.; Miesnieks, M.; Beck, T. The ethical and privacy implications of mixed reality. In Proceedings of the ACM SIGGRAPH 2019 Panels, Los Angeles, CA, USA, 28 July 2019; pp. 1–2.
17. Heller, B. Watching androids dream of electric sheep: Immersive technology, biometric psychography, and the law. Vand. J. Ent. Tech. L. **2020**, 23, 1.
18. Ríos-Sánchez, B.; Silva, D.C.d.; Martín-Yuste, N.; Sánchez-Ávila, C. Deep learning for face recognition on mobile devices. IET Biom. **2020**, 9, 109–117. [CrossRef]
39. Cadoni, M.; Lagorio, A.; Grosso, E. Large scale face identification by combined iconic features and 3d joint invariant signatures. Image Vis. Comput. **2016**, 52, 42–55. [CrossRef]
40. Cadoni, M.; Lagorio, A.; Grosso, E. Do CNN's features correlate with human fixations? In Proceedings of the 3rd International Conference on Applications of Intelligent Systems, Las Palmas de Gran Canaria, Spain, 7–12 January 2020; pp. 1–6.
41. Naik, N.; Jenkins, P. uPort open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain. In Proceedings of the 2020 IEEE International Symposium on Systems Engineering (ISSE), Vienna, Austria, 12 October–12 November 2020; IEEE: Piscataway Township, NJ, USA, 2020; pp. 1–7.
42. Tobin, A.; Reed, D. The inevitable rise of self-sovereign identity. Sovrin Found. **2016**, 29, 18.
43. Stokkink, Q.; Pouwelse, J. Deployment of a blockchain-based self-sovereign identity. In Proceedings of the 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), Halifax, NS, Canada, 30 July–3 August 2018; IEEE: Piscataway Township, NJ, USA, 2018; pp. 1336–1342.
44. Fenu, G.; Marras, M.; Boratto, L. A multi-biometric system for continuous student authentication in e-learning platforms. Pattern Recognit. Lett. **2018**, 113, 83–92. [CrossRef]
45. Mahfouz, A.; Mahmoud, T.M.; Eldin, A.S. A survey on behavioral biometric authentication on smartphones. J. Inf. Secur. Appl. **2017**, 37, 28–37. [CrossRef]
46. Ruiu, P.; Caragnano, G.; Masala, G.L.; Grosso, E. Accessing cloud services through biometrics authentication. In Proceedings of the 2016 10th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS), Fukuoka, Japan, 6–8 July 2016; IEEE: Piscataway Township, NJ, USA, 2016; pp. 38–43.
47. Falchuk, B.; Loeb, S.; Neff, R. The social metaverse: Battle for privacy. IEEE Technol. Soc. Mag. **2018**, 37, 52–61. [CrossRef]
67. Berbecaru, D.; Lioy, A.; Cameroni, C. Authorize-then-authenticate: Supporting authorization decisions prior to authentication in an electronic identity infrastructure. In Intelligent Distributed Computing XIII; Springer: Berlin/Heidelberg, Germany, 2020; pp. 313–322.
68. Li, Y.; Zou, B.; Deng, S.; Zhou, G. Using feature fusion strategies in continuous authentication on smartphones. IEEE Internet Comput. **2020**, 24, 49–56. [CrossRef]
69. Kumar, R.; Phoha, V.V.; Serwadda, A. Continuous authentication of smartphone users by fusing typing, swiping, and phone movement patterns. In Proceedings of the 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), Niagara Falls, NY, USA, 6–9 September 2016; IEEE: Piscataway Township, NJ, USA; 2016; pp. 1–8.
70. Baggio, G.; Corsini, A.; Floreani, A.; Giannini, S.; Zagonel, V. Gender medicine: A task for the third millennium. Clin. Chem. Lab. Med. (CCLM) **2013**, 51, 713–727. [CrossRef] [PubMed]