

Journal Pre-proof

Mapping the Metaverse Minefield: A TIPS Framework for Security-Conscious Business Adoption

Srinidhi Vasudevan , Anna Piazza , Lavanya Rajendran , Sameul Duraivel

PII: S0167-4048(25)00399-2
DOI: <https://doi.org/10.1016/j.cose.2025.104710>
Reference: COSE 104710



To appear in: *Computers & Security*

Received date: 1 May 2025
Revised date: 16 September 2025
Accepted date: 14 October 2025

Please cite this article as: Srinidhi Vasudevan , Anna Piazza , Lavanya Rajendran , Sameul Duraivel , Mapping the Metaverse Minefield: A TIPS Framework for Security-Conscious Business Adoption, *Computers & Security* (2025), doi: <https://doi.org/10.1016/j.cose.2025.104710>

This is a PDF file of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability, but it is not yet the definitive version of record. This version will undergo additional copyediting, typesetting and review before it is published in its final form, but we are providing this version to give early visibility of the article. Please note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

© 2025 The Author(s). Published by Elsevier Ltd.

This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>)

Highlights:

- The TIPS (Trust, Identity, Privacy, Security) framework reveals hierarchical dependencies rather than parallel considerations in metaverse adoption.
- Trust in metaverse environments emerges from socio-technical interactions, requiring organisations to address both technical security systems and social user experience considerations.
- Avatar-based representation creates unique authentication challenges requiring security approaches beyond traditional digital platforms.
- Immersive metaverse environments introduce a crucial distinction between explicit and implicit data collection, complicating privacy protection.
- Security implementation in metaverse contexts requires balancing technical protection with user experience to avoid disrupting immersion.
- Organisations should implement metaverse security in a structured sequence: establishing foundational security architecture before addressing identity management, privacy controls, and trust-building.

Mapping the Metaverse Minefield: A TIPS Framework for Security-Conscious Business Adoption

Srinidhi Vasudevan, PhD

Anna Piazza, PhD

Lavanya Rajendran, PhD

Sameul Duraivel, PhD

Corresponding Author:

Srinidhi Vasudevan, PhD

University of Greenwich Business School

UNITED KINGDOM

Abstract

As organisations embrace immersive environment to conduct their operations the metaverse can be considered as a prominent technology that both enhance business efficiency and expose them to new security vulnerabilities that cannot be fully mitigated using traditional cybersecurity models. This study explores the adoption of the metaverse through the Trust, Identity, Privacy, and Security (TIPS) framework, emphasising the interdependencies between these security dimensions. Although prior research has examined these factors independently, little attention has been paid to their combined impact on organisational adoption of metaverse. Addressing this gap, we employ qualitative research based on thematic content analysis using Natural Language Processing (NLP) and the Natural Language Toolkit (NLTK), leveraging insights from in-depth interviews with business and IT professionals from micro & small, and medium enterprises (M/SMEs)—entities that often lack extensive cybersecurity resources yet seek competitive advantages through digital innovation. Our findings reveal a structured hierarchical dependency between Trust, Identity, Privacy, and Security (TIPS) factors in metaverse adoption contexts, going beyond just identifying interrelationships between these elements. Specifically, trust in metaverse environments is influenced by user embodiment. The avatar as identity complicates identity verification and privacy protection as digital avatars merge physical and virtual identities. Finally, the metaverse raises privacy concerns, demanding frameworks that ensure transparency and user consent. Insights from our analysis suggest organisations should prioritise security-by-design principles while balancing implementation with user experience considerations to successfully navigate the socio-technical complexities of metaverse adoption.

Keywords: Metaverse adoption; Cybersecurity; Digital transformation; TIPS (Trust, Identity, Privacy & Security) framework; Socio-technical systems; Avatar identity; M/SMEs; Immersive environments

1. Introduction

Digital business environments increasingly face sophisticated cybersecurity threats that jeopardise organisational sustainability and customer trust. As organisations pursue digital transformation—integrating emerging technologies into core business processes (Fischer et al., 2020)—they must navigate complex security challenges alongside operational improvements. While digital solutions

enhance efficiency and customer engagement (Sturgeon, 2021), they simultaneously introduce vulnerabilities that make businesses more susceptible to cybercrime (Vasudevan, 2022).

This security paradox becomes particularly pronounced with immersive technologies like the metaverse, where traditional cybersecurity approaches prove insufficient against novel threat landscape. The metaverse is an immersive, interconnected virtual environment (Waykar, 2023) that leverages technologies such as augmented reality (AR), virtual reality (VR), artificial intelligence (AI), and blockchain. As such, it represents a convergence of immersive technologies and represents a frontier for digital transformation. It establishes persistent, shared virtual environments where users interact through digital avatars that embody their identity in spatial contexts, unlike traditional digital platforms (Rafique and Qadir, 2024). In the context of digital transformation, the metaverse offers organisations opportunities to gain a competitive edge, create new revenue streams, and enhance customer and employee engagement through real-time, immersive experiences (Gupta et al., 2024; Wang et al., 2022; Shankar et al., 2025). The metaverse provides multi-layered virtual environments where users interact with digital objects, other users, and autonomous agents simultaneously (Abbas et al., 2023; Tukur et al., 2023). Unlike traditional digital platforms, metaverse environments feature complex interdependencies between hardware, software, and human actors across organisational boundaries—what Michael et al. (2023) describe as 'meshed chains in open socio-technical systems.' These interconnections create unique vulnerabilities where security breaches can propagate rapidly across the ecosystem.

Addressing these challenges requires a comprehensive framework that captures the multidimensional nature of metaverse security. Indeed, researchers have identified four dimensions that collectively determine the viability and security of virtual environments: Trust, which establishes user confidence; Identity managing digital representation; Privacy, controlling personal information; and Security, implementing protective measures (Wang et al., 2022; Gupta et al., 2024). These dimensions align with the 'fundamental pillars of the digital economy' identified by Gritzalis et al. (2019) while addressing the unique challenges presented by metaverse environments. Together, these dimensions form the TIPS framework (Trust, Identity, Privacy, and Security) providing a crucial lens for understanding metaverse adoption barriers and enablers (Hernández-Tamurejo, et al., 2025; Wang et al., 2022). Without robust TIPS measures, user confidence, regulatory compliance, and technological feasibility are compromised, hindering widespread metaverse adoption (Gupta et al., 2024; Tukur et al., 2023). Studies that explore metaverse adoption within an interconnected TIPS framework remain limited, particularly in understanding how Trust, Identity, Privacy, and Security (TIPS) factors collectively influence adoption decisions (Selvam, 2024). This gap is significant because failing to grasp the collective dynamics of TIPS factors poses challenges for organisations integrating metaverse adoption into core business operations, where decisions in one domain impact outcomes in others. Specifically, in immersive environment like the metaverse, safeguarding digital identities is critical as security, trust, and privacy interact in intricate ways. The interplay between these four factors is essential for creating resilient digital environments, as each domain reinforces and complements the others to address evolving threats and challenges (Selvam, 2024). This paper addresses this gap through a qualitative investigation involving in-depth interviews with business and IT experts from micro/small and medium enterprises (M/SMEs) - organisations that often face resource constraints yet seek competitive advantages through digital innovation. By employing thematic content analysis through Language Processing (NLP) and Natural Language Toolkit (NLTK) to analyse the narrative data, while adopting the TIPS conceptual framework, we contribute to 'reconceptualizing cybersecurity awareness toward business transformation' (Akter et al., 2022) and respond to calls for multi-stakeholder, socio-technical approaches to cybersecurity challenges. As such, we ask the question, *"How do the interrelationships between Trust, Identity, Privacy, and Security factors influence organisational decisions regarding metaverse adoption?"* Our findings provide valuable insights on how these factors interact and potentially form structured relationships that influence adoption decisions, addressing a critical gap in current understanding of metaverse security. By examining these

interrelationships in the novel context of metaverse adoption, our research contributes to cybersecurity literature by extending existing frameworks to address embodied digital interaction, implicit data generation, and the integration of security measures in the immersive, metaverse environments.

The remainder of this paper is structured as follows: Section 2 discusses the theoretical underpinnings of the TIPS framework; Section 3 outlines our qualitative methodology; Section 4 presents analysis and findings; and Section 5 presents the discussions and concludes with implications and directions for future research.

2. TIPS Framework

The Trust, Identity, Privacy, and Security (TIPS) framework provides a comprehensive conceptual approach for analysing cybersecurity challenges in complex digital ecosystems such as the metaverse. Rather than treating these dimensions as isolated concerns, TIPS recognises their fundamental interconnection within digital environments. TIPS considerations play a crucial role in the adoption and continued use of emerging technologies and digital platforms (Bussone et al., 2020, Chen and Xu, 2013, Eschler and Pratt, 2017). The framework offers a structured lens for examining how these four dimensions interact in metaverse contexts, where their interdependence becomes particularly pronounced. At its core, TIPS recognises that digital ecosystems comprise entities (individuals, groups, organisations) whose interactions are mediated through digital mechanisms that must simultaneously address all four dimensions to create sustainable environments.

In the TIPS framework, trust represents the social ties between parties where vulnerability is accepted with the expectation of appropriate behaviour (Song et al., 2025). Identity refers to the identifiers associated with users that authenticate them within systems, services, and processes in both physical and digital realms (Wang et al., 2022). Privacy concerns a person's ability to control how their data are revealed to others, which becomes particularly complex in immersive environments capturing physiological and behavioural data (Far & Rad, 2022). Finally, security addresses the protection of data against unwanted access, encompassing both conventional threats and metaverse-specific challenges like avatar hijacking (Sharma et al., 2024).

There are several pivotal technological solutions that address multiple components simultaneously, specifically in the context of metaverse and these include blockchain technology, Self-Sovereign Identity (SSI) and Zero-Trust Model. Blockchain Technology serves as foundational infrastructure for metaverse security, providing tamper-resistant, transparent, and immutable ledgers that enhance trust, secure digital identities, protect privacy, and ensure data integrity (Wang et al., 2024). Its decentralised architecture aligns with the distributed nature of metaverse environments. Self-Sovereign Identity (SSI) frameworks allow individuals to control their identity data using Decentralised Identifiers (DIDs) and verifiable credentials (VCs), enabling selective disclosure of personal information while maintaining authenticity (Wang et al., 2022; Huang et al., 2023). SSI simultaneously addresses trust (through user control), identity (through decentralised authentication), privacy (through selective disclosure), and security (through cryptographic verification). Finally, Zero-Trust Model follows the principle of "never trust, always verify," requiring continuous authentication and authorisation for system access regardless of location or network connection (Cheng et al., 2023). This paradigm enforces strict identity validation, least privilege access, and ongoing verification that supports all four TIPS dimensions in the inherently fluid metaverse environments. The interconnectedness of these dimensions is evident in how blockchain-based solutions simultaneously address trust (through immutability), identity (through Decentralised Identifiers [DIDs]), privacy (through selective disclosure), and security (through cryptographic protection). By adopting this holistic perspective, TIPS provides a structured approach for analysing the multifaceted challenges businesses face when

considering metaverse adoption, responding directly to the call for theoretical frameworks that conceptualise cybersecurity, privacy, and trust within relevant risk contexts (Al-kfairy et al., 2024).

2.1 Trust

Trust in the context of the metaverse represents a multidimensional construct that extends beyond traditional digital environments. Unlike conventional online interactions, the immersive nature of metaverse environments introduces unique dimensions of trust that span technical reliability, social validation, and institutional guarantees (Jim et al., 2023, Al-Kfairy et al., 2023). Trust in these contexts must accommodate the blurred boundaries between physical and virtual identities, persistent digital assets with real-world value, and complex cross-platform interactions. As Gritzalis et al. (2019) assert, trust constitutes one of the three fundamental pillars of the digital economy (Jelovac et al., 2022), alongside cybersecurity (Akter et al., 2022) and privacy, making it critical to sustainable business operations in emerging digital landscape.

Establishing trust in digital ecosystems such as the metaverse is both critical and complex. Traditional trust mechanisms rooted in centralised authorities are increasingly inadequate in decentralised environments where such entities are absent. Further reinforcing trust are reputation systems, which are increasingly being developed on blockchain infrastructures. These systems can evaluate the credibility of users based on their past behaviour, encouraging self-regulation and deterring malicious actors (Gebre et al., 2024). For example, a Blockchain-Based Reputation Management Framework (BBRMF) might issue trust credentials as non-fungible tokens (NFTs), reflecting dimensions such as reliability and trustworthiness (Song et al., 2025).

Despite these technological advancements, the metaverse presents unique trust challenges that businesses must address (Koohang et al., 2023). The immersive and persistent nature of metaverse environments creates novel vulnerabilities in user-to-user trust relationships, particularly when participants engage in economic transactions involving digital assets (Jin, 2024). The absence of standardised governance frameworks across metaverse platforms further complicates trust establishment, as users must navigate inconsistent policies and verification mechanisms. Additionally, the integration of physical and virtual identity representations introduces complex questions about authenticity and accountability that traditional trust mechanisms struggle to address, requiring organisations to develop metaverse-specific trust protocols that can bridge this reality gap (Dwivedi et al., 2022).

2.2 Identity

Identity is central to the security and functionality of digital ecosystems, particularly within immersive platforms like the metaverse. The concept of digital identity has evolved significantly from simple username-password combinations to complex, multi-layered representations in virtual environments (Salmony, 2018). Unlike traditional web systems, the metaverse relies heavily on persistent, portable, and secure identities represented by digital avatars (Zhao et al., 2023).

Crucially, authentication mechanisms especially multi-factor authentication (MFA) and biometric verification are evolving to address impersonation threats. Researchers have proposed continuous authentication frameworks that tie a user's physical identity to their avatar through ongoing behavioural analysis, with edge devices collecting data and deep learning models validating it server-side (Han et al., 2025). Interoperability across platforms is another key requirement. Without it, users would need to recreate identities for each virtual space. Here, blockchain-based SSI solutions offer a promising path to universal identity systems, allowing seamless navigation across different digital environments (Huang et al., 2023).

More specifically, in the metaverse context, identity takes on additional dimensions as users navigate between physical and virtual representations of themselves (Saker and Frith, 2022). For organisations, this presents unique verification challenges as they must balance security with user experience, particularly when metaverse platforms are used for business operations. Traditional enterprise identity management systems are often ill-equipped to handle the fluidity and complexity of metaverse identities, where a single user might maintain multiple context-specific avatars across interconnected platforms (Horppu and Närvänen, 2024). This multiplicity creates verification hurdles that extend beyond technological solutions to organisational policy and governance concerns (Dwivedi et al., 2022).

2.3 Privacy

Privacy in immersive metaverse environments extends beyond traditional digital privacy concepts to encompass physiological responses, spatial behaviour, and interpersonal interactions that blur the physical-virtual boundary. Privacy in digital ecosystems especially within the metaverse faces unprecedented challenges due to the volume and sensitivity of collected data, including biometric and behavioural information (Far and Rad, 2022). As users engage more intimately with virtual environments, ensuring that their data is protected from misuse becomes imperative.

Considering these unprecedented concerns relating to privacy, researchers and developers have proposed several technological and governance approaches that balance functionality with data protection. One method that is gaining traction is federated learning (FL), which allows AI models to be trained across distributed devices without transferring raw data, thereby preserving user privacy. Nevertheless, conventional FL models can struggle when applied to biometric authentication in metaverse scenarios, necessitating bespoke adaptations (Han et al., 2025).

To address this, zero-knowledge proofs (ZKPs) are being explored to enable private verification processes without disclosing actual data (Zhang et al., 2023). Advanced data governance models, such as identity-based data rights governance (IDRG), are emerging to grant users granular control over who can read or modify their content. These models are essential for managing data ownership and policy privacy in blockchain-enhanced metaverse platforms (Zhang et al., 2023). Thus, privacy concerns are fundamental pillars of the digital economy that require embedding as functional requirements from the outset. Privacy in metaverse environments encompasses not only protection of explicitly shared information but also implicit behavioural data generated through immersive interactions. The immersive nature of metaverse platforms creates unprecedented regulatory challenges as existing frameworks like GDPR were not designed with such extensive behavioural data collection in mind (Michael et al., 2019). Particularly concerning is the potential for unauthorised profiling through persistent tracking of avatar movements, interactions, and physiological responses captured through VR/AR devices, creating what Abbas et al. (2023) might characterise as a multi-layered privacy challenge requiring socio-technical responses beyond conventional data protection approaches.

2.4 Security

Security remains the bedrock of a sustainable metaverse. The ecosystem is vulnerable to both conventional threats such as phishing, broken authentication, and data injection and novel challenges like avatar hijacking, biometric spoofing, and NFT theft (Zhao et al., 2023; Sharma et al., 2024).

Several technical solutions have been researched and implemented. Robust authentication protocols such as MFA and biometric-based verification are required to secure user access. Moreover, cryptographic techniques are essential to uphold the confidentiality and integrity of transmitted data (Wang et al., 2022). Unique to the metaverse is the rise of deepfakes and mimicry attacks that exploit biometric systems. As virtual assets gain real-world value, securing wallets, tokens, and NFTs becomes a priority. Continuous authentication frameworks, like the one proposed by Han et al. (2025), add another layer of defence. By tracking behavioural biometrics and detecting anomalies, these

frameworks can swiftly identify compromised sessions or fraudulent access. Organisational strategies are also essential. Secure development lifecycles, real-time threat detection, and AI-driven anomaly analysis must be standard practice to identify breaches early and respond swiftly (Sharma et al., 2024).

Security parameters for metaverse environments must extend beyond traditional digital security boundaries to address the complex interplay between physical and virtual vulnerabilities. As such, there is a need for "evolving models of cybersecurity to respond to increasingly complex threats posed by emerging technologies" (Michael et al., 2019). The metaverse represents exactly such an emerging technology, where security frameworks must evolve from perimeter-based approaches to comprehensive models that address the meshed chains in open socio-technical systems (Michael et al., 2023). This evolution requires not just technical solutions but organisational transformation in how security is conceptualised and implemented. Particularly for businesses adopting metaverse technologies, security frameworks must adapt to protect virtual assets that have real-world value while maintaining the seamless experience users expect in immersive environments (Sharma et al., 2024).

2.5 Integration of TIPS Components

In metaverse environments, Trust, Identity, Privacy, and Security components don't exist in isolation - they constantly interact and influence each other. As physical and virtual boundaries blur, these interactions create unique challenges that aren't adequately addressed by examining each component separately. The metaverse isn't just a technological platform; it's a space where relationships form and resources exchange. Drawing from Vasudevan et al.'s (2024) work on relational ecosystems, metaverse environments function as complex networks of social relationships. In these networks, participants exchange both tangible and intangible resources, creating a system where 'social agency is not only an attribute of participants, but also an attribute to the system'. This perspective helps explain why security breaches, privacy violations, and trust issues in the metaverse aren't merely technical problems - they're properties of the entire ecosystem. When designing solutions, both social and technical factors must be considered.

Organisations looking to adopt metaverse technologies must integrate TIPS considerations into their strategic planning rather than treating them as afterthoughts or purely technical concerns. This holistic approach will be essential for developing sustainable metaverse business models that users can trust.

3. Methodology

3.1 Research Methods

This research employs a qualitative, exploratory approach, which allows for an in-depth understanding of how business and IT experts within the small to medium-sized enterprises (SMEs) and micro-small medium enterprises (MSMEs) perceive the factors influencing security adoption in metaverse environments. Following the interpretive research tradition established by Myers (1997) this approach enables exploration of subjective meanings that participants attach to metaverse security considerations. More recently researchers have used qualitative approach while studying adoption of technology [see for example, Sharma & Sehrawat (2020), Karadayi-Usta (2019), Kamal (2006)]. This research focused on four components tailored to the TIPS framework. Questions shown in Table 1 were used to capture the four factors (e.g. Trust, Identity, Privacy, and Security) influencing security adoption in the metaverse through semi-structured interviews. Additionally, we also examine how industry context potentially influences the prioritisation of different TIPS factors in metaverse adoption.

Table 1. Semi-structured interviews questions to explore the TIPS framework

No	Factor	Question
1	Trust	What are the barriers for adopting Metaverse? How do trust concerns influence these adoption barriers?
2	Security	Could you please give us a positive and a negative example of metaverse? What security considerations were evident in these examples?
3	Security	How do security requirements affect these implementation costs?
4	Trust	How might increase user trust in metaverse environments impact this value?
5	Identity	How does digital identity management factor into your governance approach?
6	Privacy	How do privacy considerations influence investment decision in metaverse technology?
7	Trust	How will you build user trust throughout this service experience?
8	Identity	How does user identity and representation factor into these experiences?
9	Privacy	How might privacy concerns shape these emerging virtual cultures?
10	Identity	How does robust identity management help prevent these privacy violations?
11	Trust	What factors would increase user trust in algorithmic decision-making in metaverse environments?

12	Security	How do you approach security liability in algorithmic systems?
13	Identity	What authentication systems could prevent identity misrepresentation while preserving privacy?
14	Trust	How might these exploitations impact user trust in metaverse platforms?

The qualitative tool provides detailed, nuanced insights into complex issues such as security, trust, and privacy that cannot be fully captured through quantitative methods. Semi-structured interviews were chosen as the primary data collection method due to their flexibility in exploring participant experiences and viewpoints. This approach is ideal for studying emerging and dynamic fields like the metaverse, where predefined questions may not fully encompass all relevant concerns. Interviews provide an opportunity to explore the depth of participant knowledge and gain insights into factors that influence metaverse security adoption, such as organisational practices, individual perspectives, and industry-specific challenges. While studies have examined aspects of cybersecurity and metaverse adoption broadly (Alsharida et al., 2025; Kumar et al., 2025), the emergent nature of metaverse environments presents unique contextual factors that remain underexplored, necessitating an inductive approach. Furthermore, participants provide valuable insights into the adoption of metaverse related to TIPS, and their perceptions are shaped by organisational sectoral, and societal contexts, potentially differing from other stakeholders (Willig, 2008).

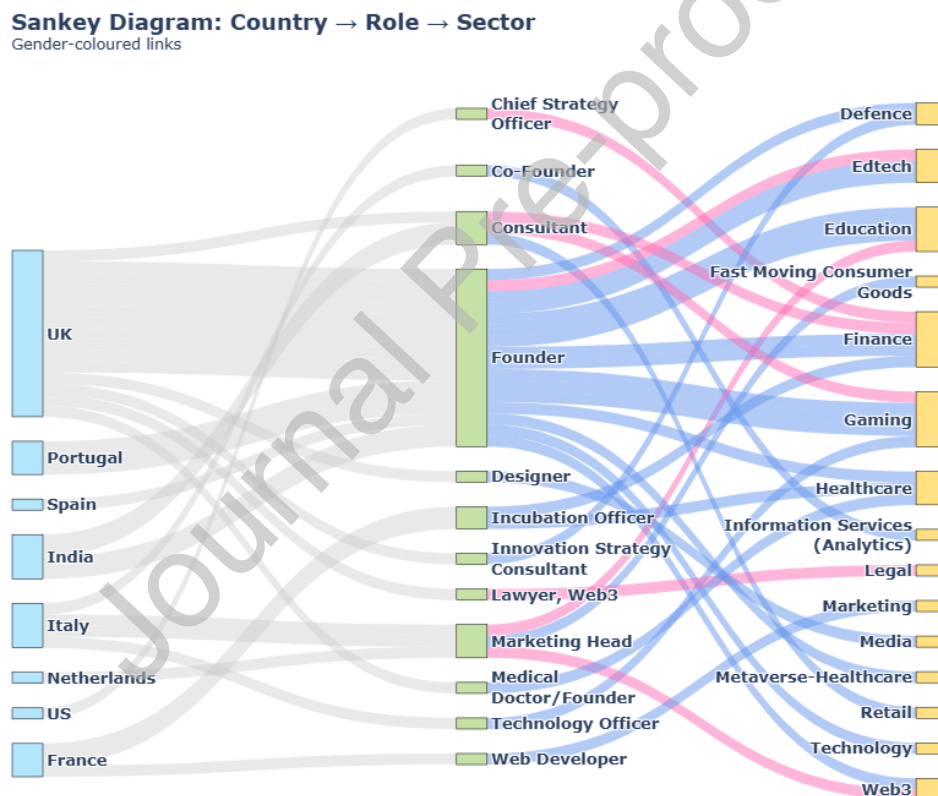
3.2 Data Collection

A total of 22 participants were interviewed. Participants were selected based on the relevance of their roles and knowledge. Our sample was diverse with consultants across multi-sector engagement highlighting cross-industry expertise. There was sectoral diversity and individuals in cross-sectoral roles emphasising interdisciplinary expertise. Organisations operate across various sectors, adopting metaverse into their business models. Interviews reached data saturation (Bekele and Ago, 2022), representing that this sample size reflects challenges and opportunities related to TIPS when adopting metaverse. Compared to other studies that have less of 22 participants (van de Weijer et al., 2024, van der Kleij et al., 2022) small and medium sizes is appropriate when participants belong to specialised sectors, have knowledge and experiences to provide valuable insight into the subject under investigation (Khan et al., 2025).

We use a mix of purposive and snowball sampling for recruiting participants from various countries with a diverse roles/background to provide a comprehensive view of security adoption across different areas the metaverse system. This sampling strategy was chosen because it allows us to use direct contacts and field interviews to gather relevant information. It is a well-established approach in qualitative research (Calandra et al., 2023) and has been used in recent studies on the metaverse (Zallio and Clarkson, 2022; Schöbel and Tingelhoff, 2023). Figure 1 represents a Sankey diagram showing the flow of participants' roles across the sector with colours capturing the gender of the participants. Specifically, the nodes represent the sectors and the roles of participants, and the flows (links) represent how roles are distributed across sectors. The line width denotes the relative frequency of the roles or sectors. The colours represent gender (Male: Blue; Female: Pink).

Following ethical approval, participants were contacted via email or direct message on LinkedIn in which we shared the aim and the purpose of the study, and their participation was voluntary. Participants have the possibility to ask any questions prior commencing, during and after interviews. The interviews started with a verbal introduction of the aim of our study followed by open-ended questions and concluded by reminded of their rights (e.g. consent, anonymity and withdraw). Interviews were conducted between March and August 2023 via Teams and lasted on average 42 with a minimum of 20 to a maximum of 60 minutes. The interviews were recorded and transcribed verbatim from the digital recordings. To ensure anonymity, all identifiable details were removed during the data cleanse and analysis and participants were labelled as ID1, ID2, and so on. The transcripts were independently reviewed by other co-authors for accuracy and confidentiality before the digital recording were deleted.

Figure 1. Flow of participants' roles across sectors with colours from roles to sectors showing the gender of the participants.



3.3 Data Analysis

The interview transcripts were processed using Python to conduct a detailed analysis of the data. This computer-assisted qualitative data analysis approach was employed to enhance analytical rigour and manage the substantial volume of interview data (approximately 733 pages of transcripts). Natural Language Processing (NLP) has been used by researchers to reduce the amount of text that needs to

be analysed by human coders and to partially automate the qualitative analysis (Crowston et al., 2012). The Natural Language Toolkit (NLTK) provides a structured collection of tools that facilitate research in computational linguistics and can be applied in qualitative research to analyse interview transcripts, assisting in thematic coding and the identification of patterns within text-based responses. Its capabilities make it a useful framework for examining how language is used in various contexts and has been applied by researchers in cybersecurity (see Marinho and Holanda, 2023; de Boer et al, 2019).

First, the transcripts were cleaned to remove extraneous elements, such as timestamps and filler words, using the `re` library. The cleaned text was then tokenized using the `word_tokenize` function from the Natural Language Toolkit (NLTK) to identify individual words. Next, a codebook was developed based on the TIPS framework, and Python was used to automate keyword identification, count occurrences of specific terms, and assign segments of the text to relevant themes. A thematic analysis approach was employed to identify, analyse, and report patterns within the data. Key themes were identified based on the frequency of relevant keywords and the contextual significance of each occurrence. The analysis was both deductive (based on the pre-defined TIPS categories) and inductive (allowing new themes to emerge from the data itself). This method allowed for a deeper understanding of the complex relationships between trust, identity, privacy, and security in the metaverse. Each interview response was analysed through the lens of the four TIPS components—Trust, Identity, Privacy, and Security—allowing us to map participants' concerns, priorities, and insights directly to these conceptual categories. This ensured a systematic approach to identifying how security adoption factors are discussed in relation to broader metaverse themes. To ensure analytical rigour, a second coder independently analysed a strategically selected 20% sample of interview transcripts, encompassing data from all sectors and participant roles. This purposive approach to validation sampling ensured verification across the full spectrum of perspectives rather than just a random subset.

To ensure the reliability and validity of the analysis, a second coder independently analysed 20% sample of the interview transcripts. The intercoder agreement was calculated using Cohen's Kappa, which resulted in a value of 0.85, indicating strong agreement between the coders. Any discrepancies in coding were discussed and resolved through consensus to enhance the consistency of the analysis.

This analytical approach enabled identification of not only individual factor importance, but also sequential dependencies between TIPS elements. The combination of frequency analysis and contextual relationship mapping revealed implementation patterns that inform both theoretical understanding and practical adoption strategies, as detailed in the following factor analysis.

4. ANALYSIS AND FINDINGS

The NLP-assisted thematic analysis revealed four distinct but hierarchically related factors influencing metaverse adoption decisions. Beyond quantifying factor mentions (Security: 120, Identity: 85, Privacy: 72, Trust: 45), the analysis uncovered dependency patterns where participants consistently described certain factors as prerequisites for others, suggesting a structured implementation sequence rather than parallel considerations.

4.1 Trust Factors

Trust emerged as a critical prerequisite for business engagement in virtual environments, with 18 of 22 participants (82%) explicitly identifying it as essential for metaverse adoption decisions. This primacy of trust manifested across three interconnected dimensions: organisational credibility, platform transparency, and demonstrated security competence. While identified as fundamental by participants, our analysis positions trust as the culmination of successfully implementing identity management and privacy controls within a hierarchical TIPS framework. This positioning emerged from participants' consistent description of trust as dependent on demonstrable security competence and transparent privacy practices. The NLP analysis revealed that trust-related discussions were invariably

preceded by identity verification or privacy protection concerns, suggesting trust functions as an outcome rather than a prerequisite in metaverse adoption decisions.

Trust was clear from the interviews as essential before adopting new technologies involving sensitive personal data and online interactions. One participant ID10: "If they [customers] don't trust us with their personal data and virtual identity, there's no reason for them to engage with our platform." Another interviewee ID20 emphasised: "Trust in the virtual space is essential—without it, businesses will hesitate to engage," underscoring that trust functions as a gatekeeper to all subsequent adoption decisions.

Our analysis revealed distinct mechanisms through which trust operates in the metaverse context. Organisational transparency emerged as a trust-building mechanism, with particular emphasis on data handling practices as outlined by ID1: "The main challenge for business is to get the credibility to work in the metaverse and to get social trust." Additionally, transparency was frequently identified as essential in building trust. The ability of organisations to be transparent about their data handling practices and to clearly communicate safety and privacy was viewed as significant for securing user confidence. Interviewee ID12 "Trust is all about openness. If users believe we are transparent about how their data is being used, they are more likely to trust our platform."

The relationship between trust and security was highlighted by respondents from technology sector who emphasised that trust is intrinsically tied to security measures. One participant ID4 noted: "To establish trust, we first need to show that the metaverse environment is secure. If users don't feel confident that their data is safe, they won't trust the platform." Another participant ID6 stated: "Without trust, users won't feel safe."

Notably, trust requirements exhibited sectoral variations, with financial services participants emphasising institutional trust mechanisms like third-party audits and compliance certifications, while gaming sector respondents prioritised community-based trust signals and reputation systems.

4.2 Identity factors

Identity verification emerged as the second most frequently discussed factor (mentioned by 19 participants), representing both a significant adoption barrier and potential competitive differentiator. The analysis revealed three distinct identity dimensions requiring attention: authentication mechanisms, avatar representation integrity, and cross-platform identity portability. This foundational element forms the basis for subsequent privacy controls and trust development within the hierarchical TIPS framework. Frequency analysis showed identity discussions often triggered subsequent privacy and security conversations, indicating identity serves as a gateway concern that activates broader security considerations. Participants consistently described identity verification as the first technical hurdle requiring resolution before addressing other TIPS elements.

Many noted the difficulty of authenticating avatars without undermining user privacy as one participant ID2 mentioned: "The primary issue in the metaverse is ensuring the identity of users, ensuring they are who they say they are". When identity solutions employ decentralised identifiers or blockchain-based credentials, firms see potential to streamline onboarding and reduce fraud, as highlighted by participant ID5: "We need a secure system that can ensure digital identity matches the physical world identity."

A prominent concern was the possibility of identity theft or fraud in virtual environments. "The metaverse needs to have a secure way to verify users' identities," noted participant ID21 especially while talking about the financial sector. On a similar note, another participant ID22 mentioned "If there's no way to guarantee that users are who they say they are, it opens the door to fraud and exploitation."

Participants identified several promising approaches to these challenges, with particular emphasis on blockchain-based verification, biometric authentication including retinal scanning and voice recognition, and reputation-based systems that leverage established digital identities from trusted platforms. Some participants pointed out that establishing a reliable identity verification system could become a competitive advantage, particularly for industries dealing with sensitive information. A participant from a healthcare ID14 stated: "If we can establish trusted digital identities in the metaverse, it will open new avenues for virtual healthcare services, as users will be confident that their personal health information is protected."

Several participants highlighted the need for avatars to reflect a secure and verified digital identity and the quote from participant ID3: "Avatars are not just characters; they are representations of real people. If we don't secure the avatar, we're leaving our users vulnerable," is a testament to it. Identity, therefore, emerged as both a challenge and an opportunity, requiring businesses to balance creating seamless experiences while implementing robust systems that ensure identity security.

4.3. Privacy Factors

Privacy considerations manifested through three distinct but interrelated dimensions: data sovereignty concerns (control over personal information), behavioural monitoring apprehensions (surveillance of avatar actions), and privacy-as-differentiator perspectives. These dimensions appeared with varying prominence across different industry sectors, with financial services and healthcare participants expressing the most acute privacy concerns. Our interviews revealed that effective privacy implementation depends on robust identity management, emphasizing the hierarchical relationship between these factors. The analysis of interview discussions revealed privacy concerns typically emerged after identity management discussions, supporting the hierarchical positioning. Participants' privacy considerations were consistently framed in relation to established identity management capabilities, suggesting privacy controls build upon identity foundations.

Business leaders expressed unease about behavioural tracking and data monetisation in immersive environments pointed out by participant ID7: "The risk of surveillance and data exploitation in the metaverse is a huge concern. It could deter businesses from adopting the technology," reported a retail sector executive. Conversely, when privacy protections are deeply embedded, organisations perceive a competitive advantage as highlighted by participant ID13: "We can guarantee privacy through blockchain, but we need to ensure users trust the system to protect their data."

The central issue identified was the difficulty in ensuring privacy when users engage with the metaverse. "One of our biggest worries is that we can't fully control what happens to our users' data once it's in the metaverse," noted participant ID9 while another participant ID11 mentioned, "If users' personal data is exposed or misused, it could lead to severe reputational damage."

Some participants saw privacy protection as a potential differentiating factor. "Privacy is something we can use to our advantage, [...] Offering guaranteed privacy protections could be a key selling point for our platform, especially in industries where data confidentiality is paramount." Said participant ID16.

Regulatory considerations significantly influenced privacy perspectives, with European participants expressing particular concerns about GDPR compliance in metaverse contexts. "Navigating GDPR requirements in the metaverse presents unique challenges—the regulation wasn't designed with immersive environments in mind, yet the data processing is more intimate and persistent than ever before." noted participant ID18.

Participants identified several promising privacy-enhancing technologies (PETs) for metaverse implementation, including zero-knowledge proofs for authentication without full identity disclosure, federated learning approaches that process data locally rather than centrally, and granular permission systems giving users unprecedented control over their digital footprint. However, these solutions were generally described as nascent rather than production-ready.

4.4. Security Factors

Security emerged as the predominant concern across all interviews, mentioned 120 times compared to 85 references to identity, 72 to privacy, and 45 to trust. The analysis revealed four distinct security dimensions: infrastructure security (platform architecture and protocols), transactional security (economic interactions), asset security (digital possessions), and interoperability security (cross-platform vulnerabilities). Our findings position security as a cross-cutting concern that both enables and reinforces all other elements in the hierarchical TIPS framework.

Participants identified potential hacking of virtual assets, vulnerabilities in transaction integrity, and the need for resilient threat-detection systems as key issues. "Security is the most important factor when deciding whether to engage with metaverse platforms. If the platform is not secure, no one will trust it," declared one participant ID15, while a web3 specialist (participant ID12) added: "We need better authentication processes to ensure that users and organisations are properly protected."

Security priorities exhibited significant sectoral variation. Financial services participants emphasised transaction integrity and fraud prevention, while retail sector respondents focused primarily on customer data protection. Education sector participants uniquely highlighted the importance of age-appropriate security controls and predatory behaviour prevention, reflecting their particular stakeholder concerns.

Participants identified several metaverse-specific threat vectors absent from conventional digital environments. These included vulnerabilities in spatial computing interfaces (mentioned by 3 participants), risks associated with persistent digital assets (8 participants), and novel social engineering attacks exploiting immersive presence (7 participants).

4.5. Integration of TIPS Elements

Analysis revealed structured hierarchical dependencies between TIPS elements beyond simple interconnection. Security emerged as foundational infrastructure enabling identity management, which in turn supports privacy controls that collectively build user trust. Indeed, the interviews revealed that businesses perceive security as the foundational element on which trust, privacy, and identity management rely. This is highlighted by participant ID13 who said: "Security is the bedrock. Without it, nothing else matters." In this view, security measures were the enablers that allow businesses to address identity and privacy concerns while simultaneously building trust with users. **Table 2** summarises the frequency of mentions of each TIPS component throughout the interviews, providing a clear visual representation of their relative importance across various sectors.

Table 2. Frequency of Mentions of TIPS Components Across All Interviews

Component	Frequency of Mentions	Key Tokens and Themes
Security	120	Data Breaches, Cybersecurity, Encryption, Platforms
Identity	85	Authentication, Digital Avatars, User Verification
Privacy	72	Data Protection, Privacy Breaches, User Data
Trust	45	Trustworthiness, Transparency, User Confidence

The analysis also revealed a hierarchical relationship between the TIPS components. Security was most often cited as the priority, followed by privacy, identity, and then trust. While trust was universally acknowledged as vital for successful adoption, businesses were primarily focused on implementing secure platforms that could later support privacy features and identity management systems.

Interconnections Between TIPS Elements and Metaverse Adoption

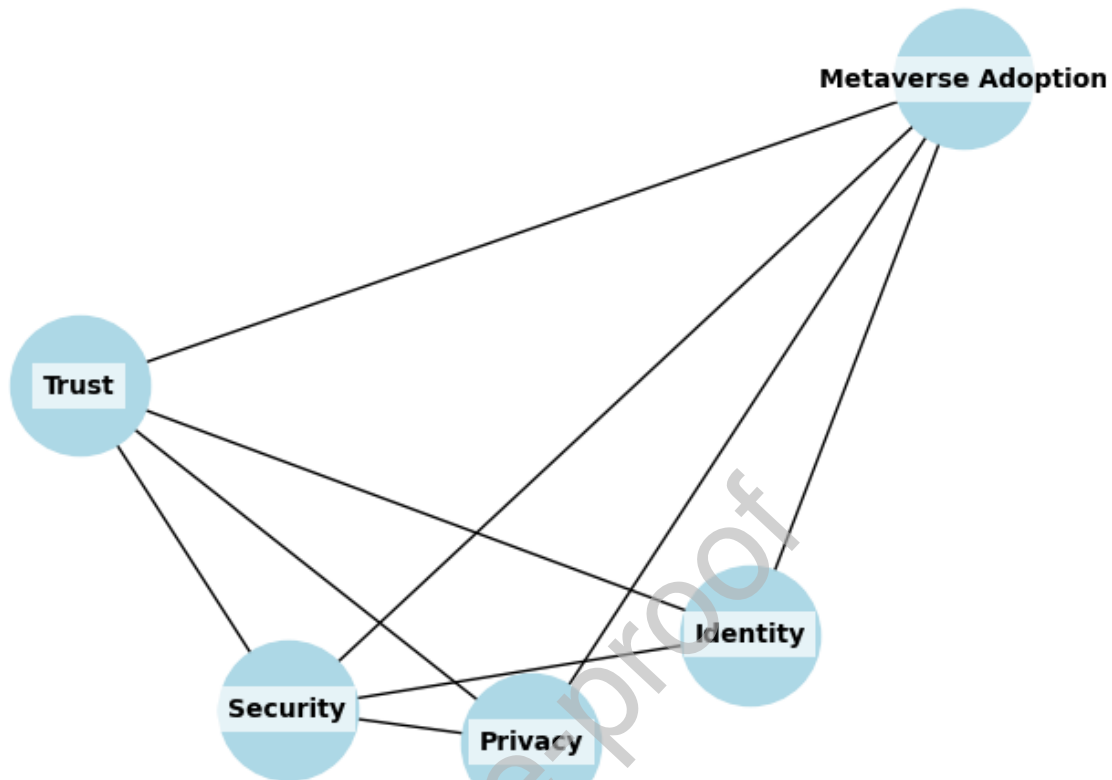


Figure 2: Interconnections Between TIPS Elements in Metaverse Adoption Decisions

Figure 2 shows the relationships between these four components. The relationships between these four components are complex, with each component influencing the others. Trust and identity management systems can only be truly effective when underpinned by strong security protocols. Similarly, businesses emphasised that privacy concerns could only be alleviated once users felt confident in the security of the environment.

These interconnections extend beyond simple co-occurrence and suggest a theoretical model where security serves as foundation, identity and privacy as enabling mechanisms, and trust as both outcome and reinforcing element.

5: Discussion and Conclusion

User embodiment in metaverse environments creates trust requirements distinct from traditional digital platforms. Participants consistently identified avatar-based interaction as requiring novel trust mechanisms addressing both technical reliability and social authenticity simultaneously.

This aligns with recent theoretical work on socio-technical systems (Malatji et al., 2019) but highlights how the spatial and embodied nature of metaverse interaction creates unique trust requirements not previously accounted for in cybersecurity frameworks. The trust-security dynamic observed in our study demonstrates what Laasch et al. (2023) describe as interdependent elements of responsible management, particularly when organisations must balance security implementation with user experience in immersive environments. Our findings demonstrate that trust in metaverse environments emerges from the interaction between technical systems (platform architecture,

security protocols) and social elements (user perception, organizational policies, cultural norms). This socio-technical interaction is particularly evident when participants described how security implementations that disrupted the flow of immersive experiences directly undermined trust, regardless of their technical effectiveness highlighting that technical security solutions must be designed with social user experience considerations at the forefront.

Avatar-as-identity paradigm generates distinctive authentication challenges requiring simultaneous verification of users' physical identity and virtual representation. Participants emphasised that traditional identity verification cannot address the spatial and embodied nature of metaverse interaction, necessitating novel approaches that maintain appropriate boundaries between physical and virtual identities.

The immersive nature of metaverse environments introduces novel privacy challenges beyond those in traditional digital platforms (Dwivedi et al., 2022). Our analysis revealed a more nuanced distinction between explicit and implicit data collection, extending privacy considerations in metaverse contexts. This represents a classic socio-technical challenge where the technical systems capturing data intersect with users' social understanding and consent processes. Our research shows that effective privacy protection in metaverse environments requires addressing both the technical architecture that enables implicit data collection and the social processes that govern transparency, consent, and user education about such collection. Unlike conventional platforms where privacy protection focuses primarily on explicit user-provided information (Clarke, 2019), metaverse environments introduce what Akter et al. (2022) would classify as a more complex privacy paradigm by capturing implicit behavioural data that users may not even recognise, they are generating. This implicit data collection constitutes what Young (2022) terms "cybercomplexity" - a situation where the boundaries between conscious data provision and ambient data harvesting become increasingly blurred. Our findings suggest that privacy frameworks for metaverse environments must account for this distinction between explicit and implicit data generation to adequately address user concerns.

Despite universal acknowledgment of security's fundamental importance, our participants described significant implementation challenges that constrain metaverse adoption. These challenges included balancing security with user experience (one participant noted that "excessive authentication steps break immersion"), managing security across interconnected platforms with varying standards, and addressing the nascent technical capabilities of current metaverse environments. Our findings reveal that security is often being retroactively integrated rather than designed into metaverse architectures from inception, consistent with observations by Schinagl et al. (2022) regarding the "security paradox" in emerging technologies.

While our research question focused on identifying interrelationships between TIPS factors, our analysis revealed a more structured hierarchical dependency that extends current theoretical understanding. A crucial contribution of our work is the sequential dependencies between Trust, Identity, Privacy, and Security elements in metaverse adoption contexts. Our findings suggest that positioning these elements hierarchically allows organisations to strategically prioritise their implementation efforts, ensuring that foundational security architecture is established before addressing more complex trust relationships. This hierarchical approach diverges from traditional cybersecurity frameworks that typically position these elements as parallel considerations (Gritzalis et al., 2019). Specifically, our findings suggest that secure and resilient identity management is a prerequisite for effective privacy controls, which in turn are essential for building user trust in metaverse environments (Fiaz et al., 2024; Alauthman et al., 2024; Yang et al., 2024).

The hierarchical model aligns with recent literature on socio-technical cybersecurity frameworks (Malatji et al., 2019) but extends these frameworks by introducing an explicit implementation sequence that recognises the interdependencies between security dimensions. This sequencing approach offers organisations a strategic roadmap for metaverse security implementation that

acknowledges both technical and social dimensions of cybersecurity as emphasised by Abbas et al. (2023). To summarise these hierarchical relationships and their empirical foundations, Table 3 presents the structured framework emerging from our analysis. This table illustrates not only how each TIPS element is positioned within the hierarchical structure but also contrasts existing literature insights with the specific empirical findings from our study. This synthesis demonstrates how our research extends theoretical understanding while providing practical guidance for organisations navigating metaverse adoption challenges.

Table 3. The hierarchical structure of the TIPS framework and its connection to the empirical findings

Element	Hierarchical Position	Role in Metaverse Adoption	Key Insights from Literature	Empirical findings from our study
Identity	Foundational	Secure user authentication and control over virtual/real identity links	Decentralised, user-controlled identity is essential to prevent PII leaks and VRIL risks (Fiaz, 2024; Yang et al., 2024)	Our interviews revealed organisations prioritise identity verification as the foundational layer before implementing any metaverse initiative. Respondents consistently identified avatar-based representation as creating unique security challenges requiring novel authentication approaches beyond traditional web contexts.
Privacy	Middle Layer	Protection of user data and behavioural information	Privacy models must build on secure identity systems to address data misuse and surveillance (Fiaz, 2024; Alauthman et al., 2024; Sharma et al., 2024; Gupta et al., 2024)	Participants emphasised the distinction between explicit and implicit data collection unique to immersive environments, with particular concern for behavioural data collected through movements, gaze tracking, and physiological responses. Our study found that organisations without robust identity management struggled to implement effective privacy controls.

Trust	Top Layer	User and organisational confidence in metaverse platforms	Trust is achieved when identity and privacy are robust, enabling safe adoption and engagement (Fiaz, 2024; Alauthaman et al., 2024; Sharma et al., 2024)	Our analysis revealed trust as emergent from successful implementation of lower hierarchical elements. Organisations reported trust could only be established after demonstrating secure identity management and transparent privacy practices.
Security	Cross-cutting	Implementation of protective measures across all layers	Security-by-design principles crucial for metaverse resilience (Austin & Withers, 2020; Samtani et al., 2020)	Our interviews revealed security implementation challenges specific to immersive environments, including balancing security with immersive experience ("excessive authentication steps break immersion") and managing security across interconnected platforms with varying standards. Security emerged as both foundational infrastructure and a continuous process that spans all hierarchical levels.

Theoretical contribution

Our study makes several important theoretical contributions to the understanding of security adoption in metaverse environments. First, the use of the TIPS framework and its empirical application to the SME, and MSMEs introduces sequential/hierarchical implementation approach that recognises the interdependencies between security dimensions. Thus, contributes to the existing literature on cybersecurity by providing a new perspective on the different but interconnected elements: trust, identity, privacy and security, that are typically investigated as parallel considerations (Gritzalis et al., 2019) rather than as sequentially dependent elements.

Temporal and sectoral implementation through Cybersecurity Capability Maturity Model

The hierarchical TIPS framework demonstrates temporal characteristics that align with organisational cybersecurity maturity progression. Through the lens of the Cybersecurity Capability Maturity Model (C2M2), we observe how the dependencies between TIPS elements evolve as metaverse technologies mature and organisational familiarity increases (U.S. Department of Energy, 2012). In nascent stages (C2M2 ML0-ML1), the absence or ad-hoc nature of cross-cutting Security leaves the foundational Identity layer highly vulnerable, leading to fragmented user representations within virtual spaces.

Privacy remains largely undefined and unprotected, with personal data collected without robust consent mechanisms. This inherent weakness means Trust is minimal and fragile, susceptible to privacy concerns. As organisations progress to managed stages (C2M2 ML2), Security becomes more pronounced and effective. With planned, documented, and consistently implemented cybersecurity practices, security actively reinforces the foundational Identity layer, enabling more reliable identity management systems, including multi-factor authentication and initial steps towards decentralised identities. This enhanced security empowers the Privacy layer, allowing consistent application of privacy-by-design principles and granular user controls. The bolstering of both Identity and Privacy, driven by mature cross-cutting security, systematically builds Trust, transitioning it from a fragile concept to tangible confidence in metaverse environments. At defined and optimised stages (C2M2 ML3), Security operates as a highly adaptive and seamlessly integrated cross-cutting element, enabling a truly robust TIPS framework. The foundational Identity layer evolves to support sovereign, contextual, and verifiable digital identities across interoperable metaverse spaces. This supreme level of Security ensures the Privacy layer can implement proactive privacy measures with advanced cryptographic techniques and absolute user control. This comprehensive integration cultivates intrinsic and measurable Trust, transforming the metaverse into a reliable, ethical, and secure digital frontier.

Our analysis revealed significant sectoral variations in TIPS prioritisation that intersect with the temporal maturity evolution described above. Financial sector participants (ID21, ID22) demonstrated a compliance-first approach where regulatory requirements shaped implementation priorities, emphasising identity verification and KYC processes reflecting organisations operating at managed C2M2 stages (ML2) where documented cybersecurity practices enable robust identity foundations. These organisations implemented Self-Sovereign Identity (SSI) systems that maintained regulatory compliance while enabling immersive client interactions. Privacy controls focused heavily on transaction confidentiality through zero-knowledge proof systems, maintaining audit trails for regulatory oversight while protecting client data. Trust-building emphasised transparent governance structures and third-party security audits, reflecting the sector's reputation-sensitive nature.

Healthcare participants prioritised privacy controls due to HIPAA (Health Insurance Portability and Accountability Act) requirements, beginning with privacy-by-design architectures before addressing identity management thereby suggesting these organisations had progressed beyond nascent stages to develop comprehensive privacy frameworks. Their TIPS implementation began with comprehensive privacy-by-design architectures before addressing identity management. Identity systems incorporated biometric authentication with behavioural analytics for session continuity while maintaining patient anonymity. Security measures emphasised end-to-end encryption for biometric data with local processing to minimise data exposure. Trust emerged through patient control mechanisms and transparent consent processes.

Educational sector participants demonstrated a trust-centric approach, prioritising community safety. Their TIPS implementation emphasised trust-building through community-based reputation systems and peer validation mechanisms. Identity management incorporated institutional credentials with behavioural biometrics to prevent academic fraud while protecting student privacy. Privacy controls included age-appropriate data collection with granular parental controls. Security focused on real-time monitoring for predatory behaviour with automated intervention systems.

These variations demonstrate that sectoral priorities influence the pace and sequence of C2M2 progression, with regulatory environments accelerating certain TIPS elements while maintaining the hierarchical structure. This also demonstrates that effective metaverse security frameworks must accommodate industry-specific priorities rather than adopting universal approaches.

This hierarchical model makes an important contribution to socio-technical systems theory by demonstrating how technical infrastructure and social dynamics interact in structured, sequential ways. Rather than treating social and technical elements as parallel considerations, our findings suggest they are hierarchically interdependent—with technical identity foundations enabling social trust processes, and social privacy expectations shaping technical implementation requirements. This reconceptualisation of the relationship between social and technical factors offers a more nuanced understanding of how organisations can navigate the complex socio-technical landscape of metaverse adoption.

Second, our findings contribute to the emergent literature on embodied digital interactions by identifying how avatar-based representation introduces unique security and privacy challenges not present in traditional digital environments. This extends Paja et al.'s (2013) work on security requirements in socio-technical systems by introducing spatial factor as a critical variable in identity management and security implementation. Third, our research advances understanding of the relationship between explicit and implicit data generation in immersive environments, contributing to what Young (2022) terms the "cybercomplexity" discourse by highlighting how metaverse environments blur the boundaries between conscious data provision and ambient data harvesting. This theoretical insight has important implications for privacy frameworks in immersive technologies. Finally, our study contributes to the literature on responsible management in technology contexts (Laasch et al., 2023) by demonstrating how the implementation of security, privacy, and identity measures in metaverse environments requires balancing competing priorities such as user experience, data protection, and technological feasibility.

Practical Implications

Our findings offer practical implications for organisations considering metaverse adoption. The hierarchical TIPS framework provides decision-makers with a structured implementation sequence recognising dependencies between security elements. Organisations should establish robust security foundations before progressing to identity management, privacy controls, and trust-building measures.

These priorities translate into specific technical considerations emerging from participants' experiences across sectors. Architecture-specific guidance includes implementing distributed identity management using blockchain-based Self-Sovereign Identity (SSI) protocols for avatar-to-user authentication, as financial participants emphasised regulatory-compliant identity verification needs. Edge computing architectures for real-time biometric processing minimise latency in immersive environments, addressing healthcare participants' therapeutic presence concerns. Federated learning frameworks for privacy-preserving behavioural analytics respond to educational participants' requirements for protecting student data while enabling learning analytics.

Protocol-level security reflects unique challenges participants identified in embodied virtual environments. Integrating WebXR security standards with Zero-Trust architectures addresses spatial metaverse interactions that participants highlighted as fundamentally different from traditional web-based models. Homomorphic encryption for computational privacy in shared virtual spaces enables collaborative environments while maintaining data confidentiality as highlighted in our interviews and something that developers need to consider. Spatial authentication protocols verifying user location within virtual environments address participants' concerns about unauthorised access to sensitive spaces.

Data handling mechanisms respond to participants' emphasis on explicit versus implicit data collection distinctions. Technical frameworks for granular consent management of implicit biometric streams (gaze tracking, haptic feedback, physiological responses) address participants' concerns about users'

limited awareness of data generation. Differential privacy techniques for aggregate behavioural analytics enable insight derivation while protecting individual privacy. This solution has been seen to be effective especially in the education sector as highlighted by our participants. Secure multi-party computation protocols for cross-platform identity verification support the interoperability participants identified as essential while maintaining security integrity.

Our research highlights designing security measures specifically for embodied interaction rather than transferring existing frameworks to metaverse environments. This addresses the current interoperability crisis where fragmented security standards across metaverse platforms create barriers to seamless user experiences and enterprise adoption. The hierarchical TIPS framework provides a standardized foundation that can resolve this fragmentation by establishing common security dependencies that all platforms must address sequentially. This necessitates a phased approach aligning technical implementation with organisational cybersecurity maturity, integrating the C2M2 framework with sectoral requirements. The technical implementation roadmap progresses through three phases corresponding to C2M2 maturity levels. Phase One focuses on Identity Foundation during C2M2 ML1-ML2 stages, deploying WebAuthn-compatible biometric authentication systems establishing secure user-avatar relationships. This includes implementing decentralised identifier standards for avatar management and cryptographic key management for virtual identity binding. Phase Two addresses Privacy Layer during C2M2 ML2 stages, integrating privacy-preserving machine learning for behavioural analysis. Confidential computing enclaves for sensitive data processing provide computational privacy essential for regulatory compliance. Selective disclosure protocols enable users to control information revelation, addressing privacy concerns in social virtual environments. Phase Three establishes Trust Layer during C2M2 ML3 stages, deploying reputation systems using verifiable credentials for community-based trust mechanisms. Smart contracts for automated trust verification provide transparent governance structures, while cross-platform identity interoperability protocols enable seamless experiences across interconnected metaverse ecosystems.

Embedding TIPS Values in Metaverse design process

Our hierarchical TIPS framework reveals that security, privacy, trust, and identity represent fundamental values requiring integration throughout metaverse design rather than post-development compliance measures. The sequential dependencies identified suggest a value-driven design approach where each hierarchical layer embeds specific ethical principles.

Security-by-design principles establish foundational values of data protection and system resilience. Identity management embeds values of user autonomy, authenticity, and control over digital representation. Privacy controls implement values of transparency, consent, and user empowerment over personal data. Trust mechanisms embed values of organisational accountability, transparent governance, and user agency.

This values-based approach transforms TIPS from technical requirements into organisational principles guiding every design decision. Participants emphasised that successful metaverse adoption required embedding these values from initial conceptualisation through deployment, rather than retrofitting security and privacy measures.

Future research

Future scholars could build and improve on our work in several ways. First, in our work we used a cross-sectional design, further researchers could employ a longitudinal design to examine how the hierarchical TIPS framework evolves as metaverse technologies mature and become more widespread in organisational settings. Second, our work used a qualitative approach to explore the quantitative interdependencies between TIPS elements, further research could use a quantitative approach to examine the framework, potentially developing measurement scales for assessing organizational

readiness for secure metaverse adoption. Finally, we investigated the perception and adoption of metaverse, further research could investigate successful metaverse security implementations and develop practical guidelines for organisations navigating the socio-technical complexities of immersive digital environments, particularly exploring how security-by-design principles can be effectively applied to metaverse architecture.

Our focus on SMEs and MSMEs may limit generalisability to larger enterprises. Future research should examine TIPS implementation in enterprise-scale deployments and conduct longitudinal studies tracking organisations through C2M2 maturity stages. Cross-cultural variations in privacy expectations and trust-building mechanisms warrant investigation across different geographical contexts. These investigations are essential for resolving the current uncertainty around enterprise metaverse deployment timelines and investment priorities, where organisations lack empirical guidance on security maturation pathways necessary for sustainable metaverse integration.

In conclusion, this study contributes to cybersecurity understanding in metaverse environments by introducing a hierarchical TIPS framework recognising sequential dependencies between trust, identity, privacy, and security elements. The temporal dimension, illustrated through C2M2 maturity progression, provides organisations with a roadmap for evolving metaverse security capabilities. Significant sectoral variations emphasise the need for adaptive implementation strategies while maintaining structural framework integrity. As cybersecurity and metaverse technologies are inextricably interwoven phenomena, shedding light on process and the four factors of TIPS dependencies may help enhance current understanding of the conditions that are more likely to support successful implementation in era of digital transformation.

References

- Abbas, R., Michael, K.; Pitt, J., Vogel, K.M.; and Zafeirakopoulos, M., 2023, "Artificial Intelligence (AI) in Cybersecurity: A Socio-Technical Research Roadmap", The Alan Turing Institute, <https://www.turing.ac.uk/news/publications/artificial-intelligence-ai-cybersecurity-socio-technicalresearch-roadmap>
- Akter, S., Uddin, M.R., Sajib, S. et al., 2022, "Reconceptualizing cybersecurity awareness capability in the data-driven digital economy", *Annals of Operations Research*, <https://doi.org/10.1007/s10479-022-04844-8>
- Ali, S., Abdullah, Armand, T.P.T., Athar, A., Hussain, A., Ali, M., Yaseen, M., Joo, M.I. and Kim, H.C., 2023. Metaverse in healthcare integrated with explainable AI and blockchain: enabling immersiveness, ensuring trust, and providing patient data security. *Sensors*, 23(2), p.565.
- Al-Kfairy, M., Alomari, A., Al-Bashayreh, M., Alfandi, O., Altaee, M. and Tubishat, M., 2023, November. A review of the factors influencing users' perception of metaverse security and trust. In *2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS)* (pp. 1-6). IEEE.
- Alsharida, R.A., Al-rimy, B.A.S., Al-Emran, M., Al-Sharafi, M.A. and Zainal, A., 2025. Predicting cybersecurity behaviors in the metaverse through the lenses of TTAT and TPB: a hybrid SEM-ANN approach. *Online Information Review*.
- Austin, G. and Withers, G., 2020. Creating social cyber value as the broader goal. In *Cyber Security Education* (pp. 99-118). Routledge.

- Bekele, W.B. and Ago, F.Y., 2022. Sample size for interview in qualitative research in social sciences: A guide to novice researchers. *Research in Educational Policy and Management*, 4(1), pp.42-50.
- Bussone, A., Kasadha, B., Stumpf, S., Durrant, A.C., Tariq, S., Gibbs, J., Lloyd, K.C. and Bird, J., 2020. Trust, identity, privacy, and security considerations for designing a peer data sharing platform between people living with HIV. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2), pp.1-27.
- Chen, Y. and Xu, H., 2013, February. Privacy management in dynamic groups: understanding information privacy in medical practices. In *Proceedings of the 2013 conference on Computer supported cooperative work* (pp. 541-552).
- Cheng, R., Chen, S. and Han, B., 2023. Toward zero-trust security for the metaverse. *IEEE Communications Magazine*, 62(2), pp.156-162.
- Crowston, K., Allen, E., & Heckman, R., 2012. Using natural language processing technology for qualitative data analysis. *International Journal of Social Research Methodology*, 15, pp. 523 - 543. <https://doi.org/10.1080/13645579.2011.625764>.
- de Boer, M.H., Bakker, B.J., Boertjes, E., Wilmer, M., Raaijmakers, S. and van der Kleij, R., 2019. Text mining in cybersecurity: Exploring threats and opportunities. *Multimodal Technologies and Interaction*, 3(3), p.62.
- Dwivedi, Y.K., Hughes, L., Baabdullah, A.M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M.M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C.M. and Conboy, K., 2022. Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International journal of information management*, 66, p.102542.
- Eschler, J. and Pratt, W., 2017, February. "I'm so glad I met you" Designing Dynamic Collaborative Support for Young Adult Cancer Survivors. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (pp. 1763-1774).
- Far, S.B. and Rad, A.I., 2022. Applying digital twins in metaverse: User interface, security and privacy challenges. *Journal of Metaverse*, 2(1), pp.8-15.
- Fischer, M., Imgrund, F., Janiesch, C. and Winkelmann, A., 2020. Strategy archetypes for digital transformation: Defining meta objectives using business process management. *Information & management*, 57(5), p.103262.
- Gritzalis, S., Weippl, E.R., Katsikas, S.K., Anderst-Kotsis, G., Tjoa, A. Min & Khalil, I. (eds) 2019, Trust, Privacy and Security in Digital Business 16th International Conference, TrustBus 2019, Linz, Austria, August 26–29, 2019, Proceedings 1st ed. 2019., Springer International Publishing, Cham.
- Gupta, R., Rathore, B., Biswas, B., Jaiswal, M. and Singh, R.K., 2024. Are we ready for metaverse adoption in the service industry? Theoretically exploring the barriers to successful adoption. *Journal of Retailing and Consumer Services*, 79, p.103882.
- Han, S., Hwang, E., Kim, Y. and Kwon, T., 2025. A Continuous Authentication Framework for Securing Metaverse Identities. *IEEE Transactions on Services Computing*.
- Hernández-Tamurejo, Á., Fernández-Fernández, M. and González-Padilla, P., 2025. Metaverse adoption and its implications for entrepreneurial innovation management: the influence of Gen Z's perception of innovation, privacy and trust. *European Journal of Innovation Management*.
- Horppu, J. and Närvänen, E., 2024. Reimagining the inevitable: how metaverse imaginaries construct understandings of privacy and surveillance. *Consumption Markets & Culture*, 27(4), pp.412-431.

- Huang, Y., Li, Y.J. and Cai, Z., 2023. Security and privacy in metaverse: A comprehensive survey. *Big Data Mining and Analytics*, 6(2), pp.234-247.
- Jelovac, D., Ljubojević, Č. and Ljubojević, L., 2022. HPC in business: the impact of corporate digital responsibility on building digital trust and responsible corporate digital governance. *Digital Policy, Regulation and Governance*, 24(6), pp.485-497.
- Jim, J.R., Hosain, M.T., Mridha, M.F., Kabir, M.M. and Shin, J., 2023. Toward trustworthy metaverse: Advancements and challenges. *IEEE access*, 11, pp.118318-118347.
- Jin, S.V., 2024. "In the Metaverse We (Mis) trust?" Third-Level Digital (In) equality, Social Phobia, Neo-Luddism, and Blockchain/Cryptocurrency Transparency in the Artificial Intelligence-Powered Metaverse. *Cyberpsychology, Behavior, and Social Networking*, 27(1), pp.64-75.
- Karadayi-Usta, S., 2019. An interpretive structural analysis for industry 4.0 adoption challenges. *IEEE Transactions on Engineering Management*, 67(3), pp.973-978.
- Kamal, M.M., 2006. IT innovation adoption in the government sector: identifying the critical success factors. *Journal of Enterprise Information Management*, 19(2), pp.192-222.
- Khan, N., Furnell, S., Bada, M., Rand, M., & Nurse, J. R. (2025). Investigating the experiences of providing cyber security support to small-and medium-sized enterprises. *Computers & Security*, 154, 104448.
- Koohang, A., Nord, J.H., Ooi, K.B., Tan, G.W.H., Al-Emran, M., Aw, E.C.X., Baabdullah, A.M., Buhalis, D., Cham, T.H., Dennis, C. and Dutot, V., 2023. Shaping the metaverse into reality: a holistic multidisciplinary understanding of opportunities, challenges, and avenues for future investigation. *Journal of Computer Information Systems*, 63(3), pp.735-765.
- Kumar, A., Shankar, A., Mehrotra, A., Yaqub, M.Z. and A. Alzeiby, E.A., 2025. Unveiling the dark and scary side of metaverse: an in-depth qualitative investigation. *Journal of Enterprise Information Management*, 38(2), pp.587-607.
- Laasch, O., Moosmayer, D.C. and Antonacopoulou, E.P., 2023. The interdisciplinary responsible management competence framework: An integrative review of ethics, responsibility, and sustainability competences. *Journal of Business Ethics*, 187(4), pp.733-757.
- Marinho, R. and Holanda, R., 2023. Automated emerging cyber threat identification and profiling based on natural language processing. *IEEE Access*, 11, pp.58915-58936.
- Michael, K., Abbas, R., and Roussos, G. 2023, "AI in Cybersecurity: The Paradox," in *IEEE Transactions on Technology and Society*, vol. 4, no. 2, pp. 104-109, June, doi: 10.1109/TTS.2023.3280109.
- Michael, K., Kobran, S., Abbas, R. and Hamdoun, S., 2019, "Privacy, Data Rights and Cybersecurity: Technology for Good in the Achievement of Sustainable Development Goals", 2019 IEEE International Symposium on Technology and Society (ISTAS), Medford, MA, USA, 2019, pp. 1-13, <https://doi.org/10.1109/ISTAS48451.2019.8937956>
- Paja, E., Dalpiaz, F. and Giorgini, P., 2013. November, "Managing security requirements conflicts in socio-technical systems", In: Ng, W., Storey, V.C. and Trujillo, J.C. (eds) *Conceptual Modeling. ER 2013. Lecture Notes in Computer Science*, 8217. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-41924-9_23
- Rafique, W. and Qadir, J., 2024. Internet of everything meets the metaverse: Bridging physical and virtual worlds with blockchain. *Computer Science Review*, 54, p.100678.

- Saker, M. and Frith, J., 2022. Contiguous identities: the virtual self in the supposed metaverse. *First Monday*.
- Salmony, M., 2018. Rethinking digital identity. *Journal of Payments Strategy & Systems*, 12(1), pp.40-57.
- Samtani, S., Kantarcioglu, M. and Chen, H., 2020. Trailblazing the artificial intelligence for cybersecurity discipline: A multi-disciplinary research roadmap. *ACM Transactions on Management Information Systems (TMIS)*, 11(4), pp.1-19.
- Schinagl, S., Shahim, A. and Khapova, S., 2022. Paradoxical tensions in the implementation of digital security governance: Toward an ambidextrous approach to governing digital security. *Computers & Security*, 122, p.102903.
- Schöbel, S.M. and Tingelhoff, F., 2023. Overcoming challenges to enable the potential of metaverse platforms: A qualitative approach to understand value creation. *AIS Transactions on Human-Computer Interaction*, 15(1), pp.1-21.
- Selvam, D., 2024. Securing Digital Identities: The Synergy of Information Technology Security, Trust, and Privacy. *International Journal of Computer Science, Engineering and Information Technology*. <https://doi.org/10.5121/ijcseit.2024.14501>
- Sharma, M. and Sehrawat, R., 2020. A hybrid multi-criteria decision-making method for cloud adoption: Evidence from the healthcare sector. *Technology in Society*, 61, p.101258.
- Sharma, S., Singh, J., Gupta, A., Ali, F., Khan, F. and Kwak, D., 2024. User safety and security in the metaverse: a critical review. *IEEE Open Journal of the Communications Society*.
- Song, X., Xu, G. and Huang, Y., 2025. A Fuzzy AHP-based trust management mechanism for self-sovereign identity in the metaverse. *Applied Soft Computing*, 174, p.112994.
- Sturgeon, T.J., 2021. Upgrading strategies for the digital economy. *Global strategy journal*, 11(1), pp.34-57.
- Tukur, M., Schneider, J., Househ, M., Dokoro, A.H., Ismail, U.I., Dawaki, M. and Agus, M., 2023. The metaverse digital environments: a scoping review of the challenges, privacy and security issues. *Frontiers in big Data*, 6, p.1301812.
- U.S. Department of Energy, 2012. *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*. [online] Washington, D.C.: U.S. Department of Energy. Available at: <https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2> [Accessed 1 Jul. 2025]
- van de Weijer, S., Leukfeldt, R., Moneva, A., 2024. Cybercrime during the COVID-19 pandemic: prevalence, nature and impact of cybercrime for citizens and SME owners in the Netherlands. *Comput. Secur.* 139, 103693. <https://doi.org/10.1016/j.cose.2023.103693>.
- van der Kleij, R., Schraagen, J.M., Cadet, B., Young, H., 2022. Developing decision support for cybersecurity threat and incident managers. *Comput. Secur.* 113, 102535. <https://doi.org/10.1016/j.cose.2021.102535>.
- Vasudevan, S., 2022, October. DeFi: A risky business or silver bullet for SMEs?. In *2022 International Conference on Cyber Resilience (ICCR)* (pp. 1-5). IEEE.
- Vasudevan, S., Piazza, A. and Ghinoi, S., 2024. Information diffusion in referral networks: an empirical investigation of the crypto asset landscape. *Quality & Quantity*, pp.1-18.

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T.H. and Shen, X., 2022. A survey on metaverse: Fundamentals, security, and privacy. *IEEE communications surveys & tutorials*, 25(1), pp.319-352.

Wang, F., Gai, Y. and Zhang, H., 2024. Blockchain user digital identity big data and information security process protection based on network trust. *Journal of King Saud University-Computer and Information Sciences*, 36(4), p.102031.

Waykar, Y.A., 2023. The Metaverse: Revolutionizing Human Society through Immersive Virtual Environments. *Journal of Emerging Technologies and Innovative Research*, 10(6), pp.2349-5162.

Willig, C., 2008. Introducing qualitative research in psychology: Adventures in theory and method account.

Young, C.S., 2022, *Cybercomplexity: a macroscopic view of cybersecurity risk*, Springer, Cham, Switzerland.

Zhao, R., Zhang, Y., Zhu, Y., Lan, R. and Hua, Z., 2023. Metaverse: Security and privacy concerns. *Journal of Metaverse*, 3(2), pp.93-99.

Zallio, M. and Clarkson, P.J., 2022. Designing the metaverse: A study on inclusion, diversity, equity, accessibility and safety for digital immersive environments. *Telematics and Informatics*, 75, p.101909.

Declaration of interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: