The Dark Side of Metaverse: A Multi-Perspective of Deviant Behaviors From PLS-SEM and fsQCA Finding

Article *in* SSRN Electronic Journal · January 2024

DOI: 10.2139/ssrn.4785285

Xinying Chew
Universiti Sains Malaysia

Victor Tiberius
Universität Potsdam

Alhamzah Alnoor
Southern Technical University -Iraq

Mark Anthony Camilleri
University of Malta

Taylor & Francis
Taylor & Francis Group

International Journal of Human–Computer Interaction

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/hihc20

The Dark Side of Metaverse: A Multi-Perspective of Deviant Behaviors From PLS-SEM and fsQCA Findings

Chew XinYing, Victor Tiberius, Alhamzah Alnoor, Mark Camilleri & Khai Wah Khaw

To cite this article: Chew XinYing, Victor Tiberius, Alhamzah Alnoor, Mark Camilleri & Khai Wah Khaw (03 Apr 2024): The Dark Side of Metaverse: A Multi-Perspective of Deviant Behaviors From PLS-SEM and fsQCA Findings, International Journal of Human–Computer Interaction, DOI: 10.1080/10447318.2024.2331875

To link to this article: https://doi.org/10.1080/10447318.2024.2331875

Published online: 03 Apr 2024.

INTERNATIONAL JOURNAL OF HUMAN–COMPUTER INTERACTION
https://doi.org/10.1080/10447318.2024.2331875

The Dark Side of Metaverse: A Multi-Perspective of Deviant Behaviors From PLS-SEM and fsQCA Findings

Chew XinYing[a], Victor Tiberius[b], Alhamzah Alnoor[c,d], Mark Camilleri[e], and Khai Wah Khaw[c]

[a]School of Computer Sciences, Universiti Sains Malaysia, Pulau Pinang, Malaysia; [b]Faculty of Economics and Social Sciences, University of Potsdam, Potsdam, Germany; [c]School of Management, Universiti Sains Malaysia, Pulau Pinang, Malaysia; [d]Management Technical College, Southern Technical University, Basrah, Iraq; [e]Department of Corporate Communication, University of Malta, Msida, Malta

ABSTRACT

The metaverse has created a huge buzz of interest because such a phenomenon is emerging. The behavioral aspect of the metaverse includes user engagement and deviant behaviors in the metaverse. Such technology has brought various dangers to individuals and society. There are growing cases reported of sexual abuse, racism, harassment, hate speech, and bullying because of online disinhibition make us feel more relaxed. This study responded to the literature call by investigating the effect of technical and social features through mediating roles of security and privacy on deviant behaviors in the metaverse. The data collected from virtual network users reached 1121 respondents. Partial Least Squares based structural equation modeling (PLS-SEM) and fuzzy set Qualitative Comparative Analysis (fsQCA) were used. PLS-SEM results revealed that social features such as user-to-user interaction, homophily, social ties, and social identity, and technical design such as immersive experience and invisibility significantly affect users' deviant behavior in the metaverse. The fsQCA results provided insights into the multiple causal solutions and configurations. This study is exceptional because it provided decisive results by understanding the deviant behavior of users based on the symmetrical and asymmetrical approach to virtual networks.

KEYWORDS
Deviant behaviors; metaverse; sociotechnical perspective; privacy; fsQCA

1. Introduction

The metaverse is a recent addition to the technological world. However, the term was first indicated in 1992 within Stephenson novel titled - Snow Crash. The novel embodied the metaverse as a space for virtual reality, which is also a new iteration of the Internet that uses blockchain and virtual reality headsets within the integration of the virtual and physical worlds (Barrera & Shah, 2023; Richter & Richter, 2023). Virtual reality simulates the real world and has advanced technical capabilities that enable new experiences for users and companies. In 2016, investments in the augmented virtual reality market amounted to $6.1 billion, and it is expected to reach $20.9 billion by 2025. By 2030 metaverse will contribute $13 trillion revenue (Barrera & Shah, 2023). The virtual reality industry has changed the technical landscape and has been considered a technological direction for the national strategy of many countries (Dincelli & Yayla, 2022; Pooyandeh et al., 2022; Sebastian, 2022; 2023). Several platforms have emerged that are considered antecedent and precursors to the metaverse, such as Linden Lab's multimedia platform, Fortnite, and Roblox. These platforms allow interaction between users within the virtual world (Damar, 2021). Many users have utilized such platforms especially in the mid-2000s, but these platforms have lack of functionality and independence. Mark Zuckerberg developed a newfound metaverse concept as an ecosystem to seamless the barriers to users amongst real and virtual worlds through simulating communal experiences (Dwivedi et al., 2022). The metaverse was created using virtual reality, mixed reality, extended reality, and augmented reality. The metaverse has transformed the traditional trend of users staring at electronic devices into users immersing themselves in headphones or gloves (Singla et al., 2022). The metaverse is an economic, social, and ecosystem that takes advantage of digital platforms to enable users to engage in activities and interactions by displaying a virtual persona represented by the creation of shared values such as avatars (Kar & Varsha, 2023). The metaverse is a 3D virtual distributed world through which all activities and interactions are carried out based on virtual reality services and equipment (Damar, 2021).

For every technology there is a bright side and a dark side. On the bright side, competition has increased among business organizations in how to leverage metaverse services in business models. Because this startling technology raises the experience of customers to check the products virtually, solving social problems, and exchanging experiences between individuals (Oh et al., 2023). In terms of the dark side of the metaverse, although there have been immersive and successful experiences in the metaverse, it has witnessed challenges at the level of legal and privacy matters. Challenges have increased in the metaverse that discourage

CONTACT Alhamzah Alnoor alhamzah.malik@stu.edu.iq School of Management, Universiti Sains Malaysia, 11800 Pulau Pinang, Malaysia

real-time interactions between users and eliminate engaging, immersive, and satisfying experiences (Flavián et al., 2023). Many constraints appear with the development and increasing use of metaverse technology. The negative effects of the metaverse can be dire unless controlled and managed wisely. Darkverse is considered the most accurate term to explain crimes practiced within the virtual context and via the Internet. The negative consequences and harmful effects of the metaverse include psychological, legal, security, and physiological impacts. Therefore, major concerns arise in the context of the metaverse, including the risks of addiction, exploitation, traumatic effects, harassment, and terrorism (Dwivedi et al., 2023). Deviant behaviors in the metaverse can create an unhealthy and unsafe environment for users. Exposure of vulnerable users to deviant behaviors in virtual worlds causes psychological, negative consequences, and real physical harm (Tugtekin, 2023).

Metaverse users may face a range of challenges and threats, including social, legal, ethical, security, and privacy. The growing literature on the metaverse is preoccupied with the bright side and disregard the dark sides of the metaverse (Belk et al., 2022). Metaverse research is mostly conceptual in nature (e.g., Buhalis et al., 2022; Dwivedi et al., 2022; Go & Kang, 2023; Wong et al., 2023). However, there are a few exceptions. In examining the dark side of the metaverse, Flavián et al. (2023) investigated the negative effects of the metaverse on users' experiences of a virtual cultural event. Gamification elements reduce negative effects and improve user experiences. In addition to the effect of affective states on perceived authenticity and ease of imagination. The exploration aspect of the metaverse is still incomplete and draws from historical data. Information systems experts and scholars have provided different perspectives (e.g., Dwivedi et al., 2023). On the other hand, the bright side of metaverse studies take advantage of multiple theories to explain the adoption of this technology (Gao et al., 2023). Previous literature investigated metaverse adoption by utilizing six theories, technology acceptance model (Akour et al., 2022; Almarzouqi et al., 2022), unified theory of acceptance and use of technology (UTAUT) (Arpaci et al., 2022; Teng et al., 2022), social cognitive theory (Alvarez-Risco et al., 2022), uses and gratifications theory (Hassouneh & Brengman, 2014), theory of planned behavior (Yeap et al., 2016), and virtual liminoid theory (Jung & Pawlowski, 2014). The metaverse topic needs more exploration and investigation. Therefore, the previous literature explored the determinants of social sustainability of the metaverse (Arpaci et al., 2022; Arpaci & Bahari, 2023), and metaverse adoption (Akour et al., 2022). Previous literature reported on the positive side of applying the metaverse and achieving experiencing value and practical values for virtual world experiences (Gao et al., 2023). The dark side of the metaverse is captured from two perspectives: the user perspective and the social perspective. In terms of artistic design, weak artistic design is considered a source of limitless problems and deviant behaviors. Without legal obligation and principles, the metaverse would be a different world. Users can create separate identities and engage in extremely heinous behaviors that violate the legal and ethical security of virtual platforms. Therefore, the technical and social aspect is vital in controlling deviant behaviors (Flavián et al., 2023).

The literature has sparked buzz with opportunities for metaverse users by highlighting users' interaction with digital objects, immersing themselves in social interactions, providing immersive merchants, and expanding physical experiences. However, previous studies on metaverse are fragmented and scant because it has limitless opportunities, excitement, and considered as a black box. Previous and ongoing literature contains many gaps. Firstly, understanding the deviant behavior of users in the metaverse is limited (Dwivedi et al., 2022). Secondly, the literature on sociotechnical perspective and deviant behavior in the metaverse is inconclusive. It requires a thorough investigation to understand the phenomenon by using privacy and security (Cheung et al., 2021). Accordingly, there remains a necessity to present a beyond widespread depiction that involves the dark and bright aspects of metaverse in the deviant behavior context. Third, previous studies have focused attention on users' engagement in metaverse use to determine behavioral patterns of use (Albayati et al., 2023; Lee et al., 2023). Investigation and exploration into the deviant behavior of metaverse users to expand positive repercussions and mitigate negative consequences merits study.

Metaverse has brought dangers to society and various cases of sexual harassment, hate, racism, bullying, gambling and a number of deviant behaviors have been reported in the metaverse (Li et al., 2022). There are several reasons for the prevalence of deviant behavior in the metaverse. For example, ethical and legal issues are still unresolved in the metaverse because of poor exploration of the concept of ownership and assets of this pioneering technology (Kostick-Quenet & Rahimzadeh, 2023). Online disinhibition is also considered a psychological situation that increases the feeling of comfort to increase deviant behaviors (Cheung et al., 2021). The literature calls for ongoing and future research to address the deviant behaviors of the metaverse (Cheng et al., 2022). Dwivedi and his colleagues called the authors to address the deviant behavior of the metaverse by investigating social and technical factors. Understanding the metaverse in terms of user behavior sheds light on addressing negative behaviors and increasing engagement in use (Al-Sharafi et al., 2023; Khaw et al., 2022; Lyu, 2023; Wider et al., 2023). The sociotechnical perspective is central to the coherence of the information system. Combining social and technical advantages in studying users' behaviors towards the metaverse contributes to understanding deviant behaviors (Sarker et al., 2019). The technical perspective develops users' psychological states that stimulate users' interactions, whether deviant or positive behaviors. Virtual reality technologies have also increased sensory experiences, which have led to sexual harassment behaviors appearing real in the virtual world (Dwivedi et al., 2022). The investigation of user behavior in the metaverse is still under development due to a large ambiguity and lack of literature investigating deviant user behavior (Barrera & Shah, 2023). Sociotechnical perspective influences the emotion, attitudes, and behaviors of users (Abbas et al., 2023; Abdullah et al., 2023; Sadaa et al., 2022). The metaverse is a social technology platform, sociotechnical perspective contributes to understanding users' deviant behaviors and identifying the causes and solutions for such deviant behaviors (Preece et al., 2022; Wan et al., 2017).

The literature findings on deviant behavior in the metaverse are still inconclusive. This study is a milestone for academics and practitioners to address deviant behavior. Hence, there are three main objectives of this study. First, investigate the impact of social factors (i.e., User-to-user interaction, homophily, personal traits, self-efficacy, social ties, and social identity) on users' behavior of metaverse. Second, discover the impact of technical factors (i.e., Immersive experience and invisibility) on users' behavior of metaverse. Third, explore the mediating role of privacy and security factors on the relationship between technical, social features, and users' behavior of metaverse. Last but not least, ongoing business models rely on statistical models that capture causal relationships such as PLS-SEM. PLS-SEM approach describes the exploration and testing of theories. Focusing on empirical studies towards a single statistician that does not meet business needs (Ali et al., 2023). To this end, our research is a response to calls for utilizing asymmetrical testing to understand complex events such as deviant behavior in the metaverse, social and technical features, security, and privacy by assuming that equifinality, synergistic, and nonlinearity examines among constructs exist. This research uses PLS-SEM and fsQCA to determine the true effect of each predictor on the consequence and establish their respective causal configurations (Pappas & Woodside, 2021). The application of complementary techniques to SEM has become a new direction for many research and studies. Integration of the fsQCA analysis with SEM captures the relevance of the investigative work to expected results (Abbasi et al., 2022). Utilizing fsQCA analysis in the present work would allow to investigate the joint effect under the assumption of asymmetric correlations amongst the studied variables and the intended result. The phenomena of the social sciences are becoming increasingly complex. Limited reliance on single analysis reduces the research's theoretical and practical implications (Rasoolimanesh et al., 2021). To exhibit research with conclusive findings that address the issue of deviant behavior in the metaverse, combining fsQCA and PLS-SEM deciphers complex causal mechanisms. First, SEM analysis captures causal and linear relationships to investigate the impact of technical and social features on the deviant behavior of metaverse users. Second, the fsQCA analysis identifies configurations that lead to higher or lower levels of deviant behavior based on sociotechnical perspectives, privacy, and security. Using fsQCA suggests many benefits, including capturing many of the conditions for a particular event or outcome to occur. The fsQCA creates a bridge between quantitative and qualitative aspects because such analysis uses both qualitative and quantitative assessments. Many methods suffer from the problem of variability and limitations, while fsQCA focuses on complex relationships between results. The fsQCA calculates multiple solutions for industry and academia and forms multiple, independent solution sets, as illustrated in Figures 1 and 2 (Pappas & Woodside, 2021).

2. Literature review

2.1. Deviant behaviors in the metaverse

Online disinhibition is a major cause of deviant behavior in online applications (Dwivedi et al., 2022). Disinhibited online behaviors are divided into toxic and benign disinhibition. In terms of benign disinhibition, users share their personal life details about their well-being and selves. Users use their inner selves, and this helps to solve personal problems. On the contrary, toxic disinhibition increases the behavior of users in spreading hate, racial discrimination, and cruel comments (Cheung et al., 2021). Online disinhibition is a psychological state that motivates users to do and display deviant behaviors in virtual and online applications, more than displaying them in offline situations (Wong et al., 2018). Online disinhibition makes metaverse users less restrictive. Online disinhibition is a major factor in the spread of uncivilized behavior through the Internet and virtual context (Hollenbaugh & Everett, 2013). Deviant behavior is behavior practiced by users by violating values and standards in a way that harms other users in the virtual environment (Dwivedi et al., 2023). These behaviors can range from relatively minor violations such as misuse of time and resources to major violations such as sexual harassment, vandalism, verbal and physical abuse, gambling, terrorist operations, and so on (Chu & Chau, 2014). Virtual technologies have spread around the world, with more than 4 billion people using the Internet. Information systems activities have become ubiquitous in our daily lives. Although there are many good avenues provided by virtual reality systems and information and communication systems, deviant behaviors are overshadowed because of the lack of users' restriction in such systems (Statista, 2023). The deviant behaviors practiced in online applications are sexual harassment, hatred, rumors, aggression, escalation, and bullying. Lack of restriction in augmented virtual reality is a fundamental reason for 37% of users to experience deviant behavior online (Cheung et al., 2021). Users' activities in virtual reality are characterized by a feeling of relaxation and a willingness to practice and engage in deviant behaviors that are hostile to other users and disturb them (Wright et al., 2019). Technology contributed to society's absorption of globalization. However, people's fondness for technology increases users' engagement in deviant behaviors that amount to cybercrime (Chew et al., 2023; Muhsen et al., 2023). Deviant behavior via the Internet and virtual reality technologies is a violation of Internet standards. For this result, the deviant behavior was not limited to physical damage, but also included widespread virtual damage (Zhou et al., 2022). Virtual reality technologies are simulations of reality. Protecting users in virtual reality from deviant behavior is a path to the success of virtual applications around the world.

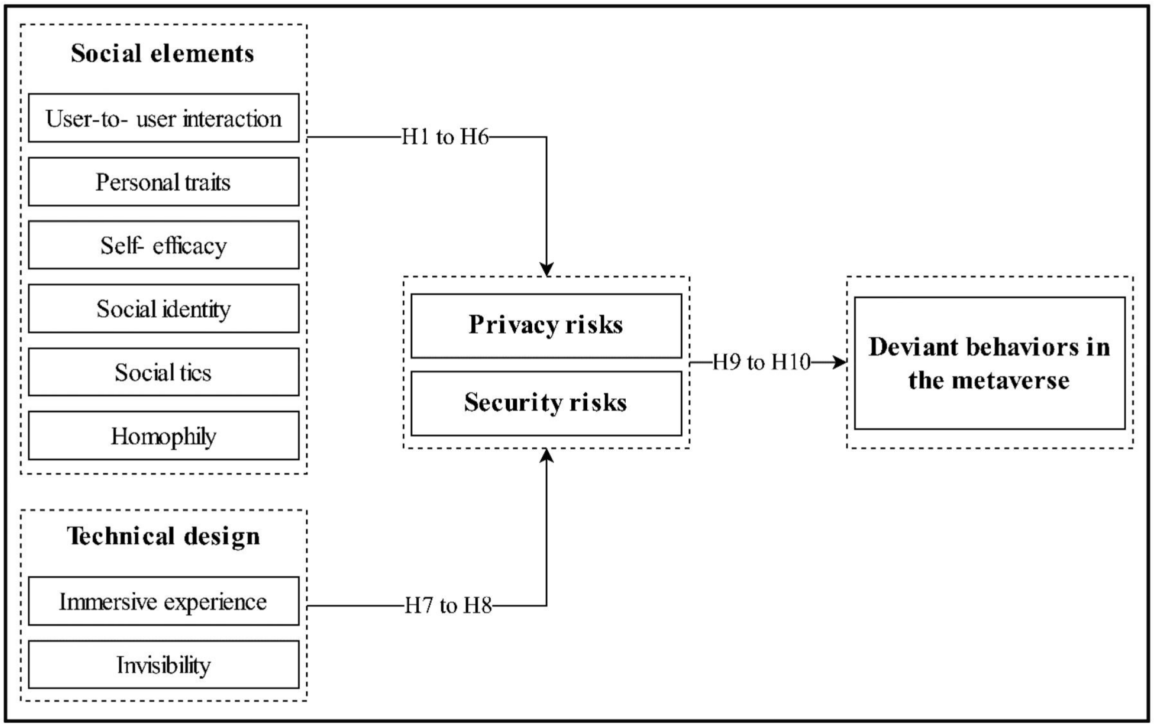

Figure 1. Conceptual framework..

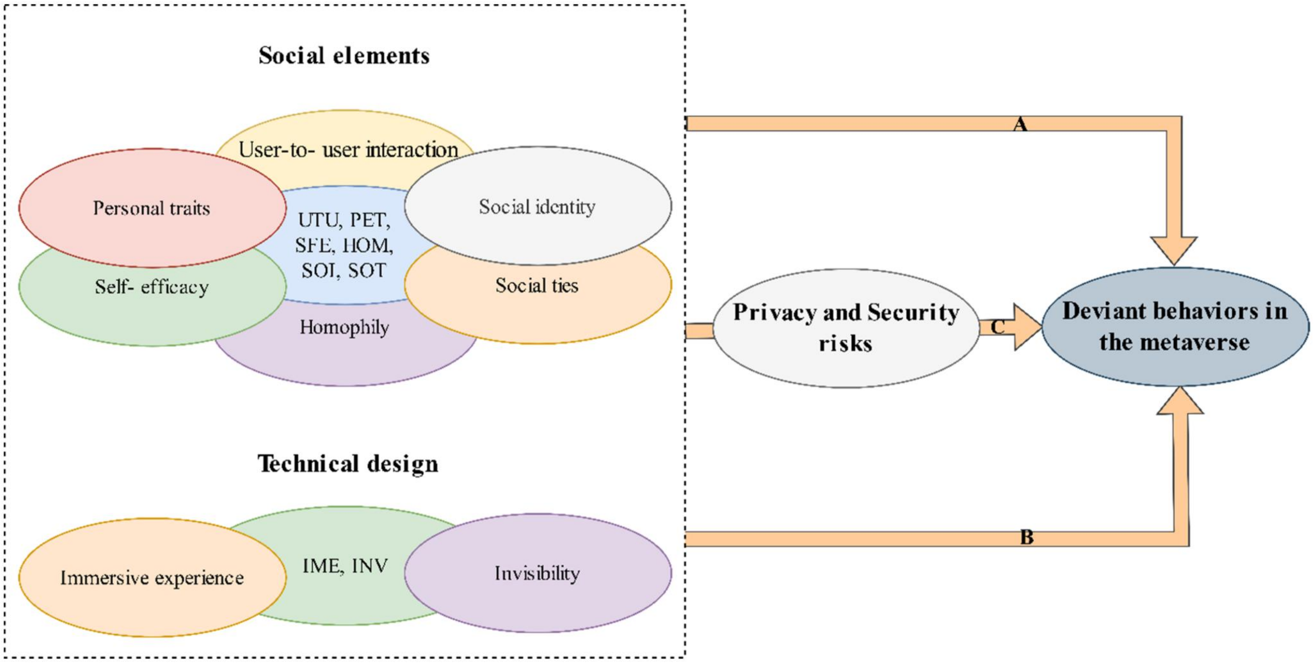

Figure 2. Configuration model.

2.2. Sociotechnical perspective

Bostrom and Heinen (1977a, 1977b) introduced the sociotechnical perspective, which assumes that information technology systems consist of social and technical subsystems. The technical subsystem is concerned with technical competence in contrast to the social subsystem which is focused on the human perspective. The social and technical subsystems work in high compatibility, and the information system is affected by the technical and social characteristics (Zhang et al., 2022). A sociotechnical perspective has been applied to virtual reality applications and research to determine the critical role of combining social activities with digital technology in driving negative outcomes such as deviant behavior and positive outcomes such as engagement in the metaverse (Kapoor et al., 2021; Zhang et al., 2019). The social technical perspective confirms that the information system consists of technical and social features that motivate users to engage in different interactions and behaviors in the metaverse. The combination of technical and social advantages serves as a shining avenue for academics and practitioners to understand engaging and deviant behavior in the metaverse. The sociotechnical perspective presents research opportunities and an interesting avenue in order to preserve the virtual world from disruptive behavior, enhance security, and augment privacy (Dwivedi et al., 2022). The sociotechnical perspective is an established framework in the information systems research landscape (Sarker et al., 2019). Users' engagement in the metaverse is related to users' perceptions of the metaverse context. In addition, the technical element is seen as an important feature, for example, when the user's avatar in virtual reality is similar to the user's personality in reality the users' confidence in interaction with other would be increased. Artificial intelligence technologies such as virtual reality are social and technical systems (Sartori & Theodorou, 2022). Scholars have proposed several factors for the sociotechnical perspective. Figure 3 summarizes the components of the sociotechnical perspective.

Figure 3 shows that there are several components of the sociotechnical approach. Zhang et al. (2022) argued that the social approach consists of active control and synchronicity while the technical approach includes visibility and personalization. However, Suh & Cheung (2019) points out that the technical perspective involves interactivity, controllability, privacy setting, ease of use, portability, and compatibility. In addition, social aspects incorporate user interaction, perceived contingency, social accessibility, social acculturation, social capital affinity, social enhancement, social identity, and social ties. Furthermore, Lee et al. (2006) claimed social components contain personal interest and social context, but technical components include technological attributes. As Cheung described metaverse from the sociotechnical perspective. Metaverse is a mixture of technical elements such as immersive experience, invisibility, and the social components such as user-to-user interaction, personal traits, self-efficacy, social identity, social ties, and homophily (Dwivedi et al., 2022). The sociotechnical approach is effective for explaining the behavior of users. The social features of virtual reality are reflected in the fact that virtual reality provides exciting opportunities for users to interact and communicate in real time. Such interactions create immersive experiences for communication and interaction between users. In contrast to the social approach, the technical approach provides a focus on technical competence and provides a visual scenario for users (Preece et al., 2022). Therefore, the technical sub-system is complementary to the social sub-system because the coexistence of technical and social features is an essential feature of virtual reality (Pedram et al., 2021). Dwivedi and his colleagues in their opinion paper about "Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy" confirmed to study of how the social components (e.g., User-to-user interaction, homophily, personal traits, self-

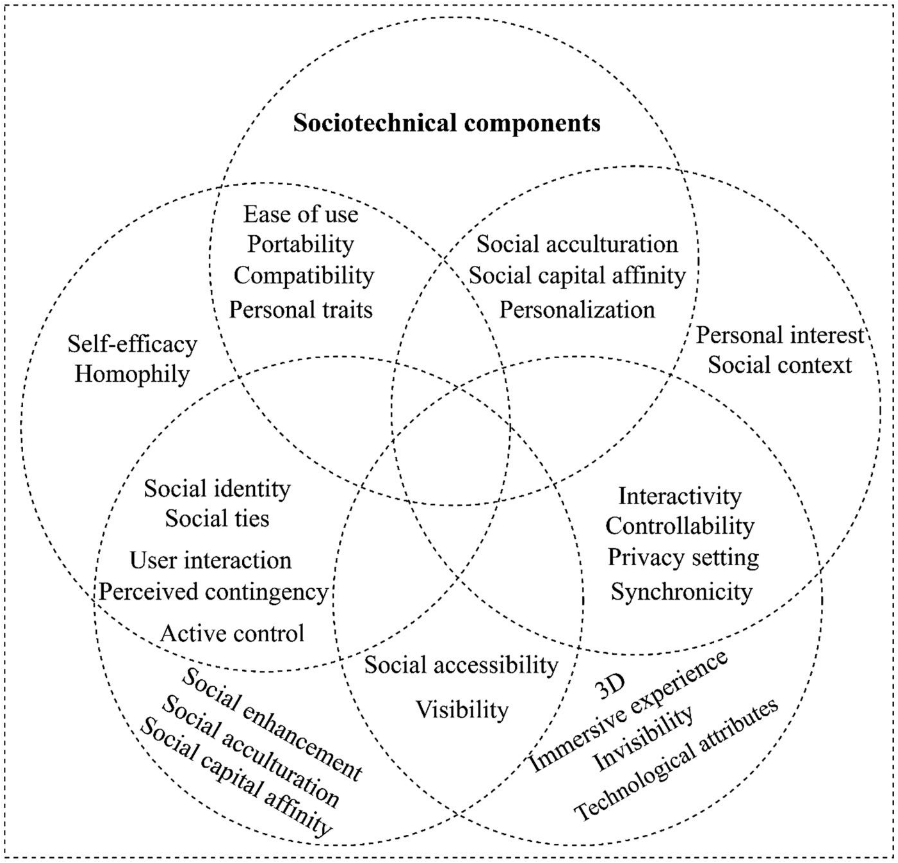

Figure 3. Components of the sociotechnical perspective.
Source: Author adopted from (Dwivedi et al., 2022; 2023; Lee et al., 2006; Suh & Cheung, 2019; Zhang et al., 2022).

efficacy, social identity, and social ties) and technical components (e.g., Immersive experience and invisibility) encourage deviant behaviours in the metaverse (Dwivedi et al., 2022). Sarker et al. (2019) claims that the mentioned sociotechnical components represent an umbrella for all technical and social factors. Therefore, previous arguments in the literature emphasize the necessity of using such components when investigating user engagement or behavioral engagement (Suh & Cheung, 2019). Understanding deviant behaviors in the metaverse by studying social factors in isolation from technical factors is not enough to reduce virtual reality risks. However, as noted previously, academics have over-investigated user engagement in the metaverse with a focus on a single side, whether social or technical. In addition to the scarcity of literature and the lack of conclusive evidence on the treatment of deviant behaviors in virtual reality applications by improving privacy and enhancing security. To this end, investigation and delving into such an issue provide rigorous evidence.

3. Hypotheses development

3.1. Social features effect on security and privacy

User-to-user interaction influences privacy and security logos and attracts users' attention when making important decisions. User interaction represents proactive displays of privacy and security notifications by providing sufficient information to identify fraudulent and legitimate websites and virtual channels. Interaction between users helps reduce uncertainty in virtual location applications and make informed decisions (Dang et al., 2020). Social elements (e.g., User-to-user interaction) advance deviant behaviors in the metaverse (Dwivedi et al., 2022). Interactions between users influence the behavior and intentions of users across social and virtual networks. Users tend to form bonds with others who have similar values and designated respect. Interaction between users in virtual networks reaches its climax due to the exchange of many types of links, posts, and media. In the absence of security and privacy, misleading and bad information can be exchanged and aggressive behaviors towards other users may be practiced (Ferreyra et al., 2022). Online platforms, including virtual platforms, are considered front lines for users to interact with each other. Sharing reliable knowledge and information online with peers increases the bonds of safety and privacy. Providing informational and emotional support contributes to developing strong interactions between users, built on strong bonds of privacy and security (Tseng, 2023). While social characteristics are powerful drivers of interaction between users and important antecedents for users engaging in deviant behavior across virtual networks (Suh & Cheung, 2019). As such, the following hypotheses are proposed:

H1a: *User-to-user interaction has a significant impact on privacy.*

H1b: *User-to-user interaction has a significant impact on security.*

Users interacting with virtual technologies such as the metaverse produce unlimited amounts of information that are exploited for various purposes. One of the factors that control the privacy and security of information in virtual networks is homophily. The association of similar people with each other is a common social feature in virtual and social networks (Ertug et al., 2022). Homophily affects users' interaction patterns because it is an intrinsic aspect of users' lives. Joining a particular group in a virtual network or performing various activities is important to profile users. The creation of a social file that contains user information in virtual networks faces the risk of abuse by toxic users (De Salve et al., 2018). Homophily is associated with the privacy and security of users by increasing the chances of disclosure of personal information and leakage of personal information (Zhang et al., 2017). Previous literature has investigated homophily's nexuses to the security and privacy of users with common habits such as interaction patterns and temporal patterns or similar preferences such as products, services, and interests among users. For example, homophily can be measured among users in metaverse platforms that contain information based on profiles. Activities conducted on virtual networks provide vital information to characterize users, which increases security and privacy risks (Dwivedi et al., 2022). Homophily impacts the privacy and security of virtual networks in various ways, including exposure of a profile through targeted advertising campaigns, implementation of a product recommendation, and prediction of engagement or behavior (Zhang et al., 2017). Homophily is used to extract and capture information that users want to protect, which exposes users to high security and privacy risks by revealing personal information and data. Understanding homophily helps protect against leaking and predicting personal information. Thus, we assume that:

H2a: *Homophily has a significant impact on privacy.*

H2b: *Homophily has a significant impact on security.*

Users of virtual networks are characterized by many personal traits. For example, agreeableness is a trait that reflects compatibility and harmony with social norms and customs. People with high agreeableness tend to get along and trust others in virtual networks. Therefore, agreeableness people care about privacy and security features more than others in terms of information disclosure and misuse (Tang et al., 2021). People with neuroticism tend to spread anxiety, disturbance, and view negative events in virtual networks (Ali et al., 2024; Kareem et al., 2024). The neurotic person is concerned with issues of security and privacy in assessing the risks of virtual networks and Internet networks (Spector et al., 2000). Conscientiousness means achievement, discipline, and competence and is associated with predictability. People with such personality traits are more vigilant and cautious about security and privacy. Neurotic people have a degree of sensitivity towards protecting personal privacy and security (Khedhaouria & Cucchi, 2019). An open personality is characterized by confidence, enthusiasm, happy experiences, and activity. Being open requires interacting with other users on virtual networking platforms and sharing a lot of information. Moreover, extroverted people are less concerned about security and privacy risks and such issues do not deter them. Extraversion or openness reduces users' concerns about security and privacy. People with high openness are characterized by a high spirit of risk, imagination, interest in unconventional matters, and willingness to reveal personal information. However, openness enables highly experienced people to deal with emerging security and privacy issues or risks (Tang et al., 2021). Furthermore, we believe that:

H3a: *Personal traits have a significant impact on privacy.*

H3b: *Personal traits have a significant impact on security.*

Confidence in self-efficacy by users increases taking appropriate precautions and measures to activate privacy protection behavior and increase security for users of virtual networks. Users' belief in cognitive resources and abilities reflects the concept of self-efficacy. People with high self-efficacy practice and engage in highly proactive behaviors to protect security and privacy (Hichang, 2010). Self-efficacy is a distinctive feature of behaviors, thoughts, and feelings about people. For example, people with agreeableness trait tend to others, comply with orders, and pay attention to delinquent behaviors. Gentle and neuroticism people care about privacy by evaluating risk in virtual networks. While simple personal users are less likely to check privacy and security conditions. On the level of conscientiousness, which is described as self-efficacy, people are more careful and sensitive to protecting personal privacy (Tang et al., 2021). People with high self-efficacy are characterized by information sharing behavior and are less likely to hide information and data via virtual networks compared to people with low self-efficacy. Self-efficacy complexes affect privacy and security behavior, but in different directions (Chang et al., 2022). Hence, the following hypotheses are proposed:

H4a: *Self-efficacy has a significant impact on privacy.*

H4b: *Self-efficacy has a significant impact on security.*

In terms of social ties, which express the relationships between users in virtual and social networks. The use of virtual and social networks is associated with social ties in the processes of use. Social ties enhance users' enjoyment and confidence in virtual platforms and reduce users' anxiety about privacy and security breaches. Interaction between users in virtual reality provides a sense of coexistence, which creates an atmosphere of pleasure that relieves users' fear of breaches of privacy and security (Lee et al., 2019). The extent to which users' engagement in interactive activities, whether good or bad, is considered a psychological state that increases the user's passion or enthusiasm towards the uses of the information system. Social ties facilitate interaction between users and control privacy. Technical advances in virtual networks have made sexual harassment and lewd behavior through virtual networks. Especially since the metaverse has reshaped the landscape of our daily lives. Social ties point of view maintains immersive experiences and secure virtual agents and networks for users and the public (Zhang et al., 2019). Furthermore, the following hypotheses are assumed:

H5a: *Social ties have a significant impact on privacy.*

H5b: *Social ties have a significant impact on security.*

Social identity explains users' behaviors in real and reality contexts. Virtual networks offer ample opportunities to share discussions, post comments, and report on experiences, creating a shared sense of identity and developing shared norms and values. Virtual networks snap opportunities for users to develop a social identity. Privacy and security risks have prompted users to reconsider their accounts and changed the way users reveal themselves because security and privacy have undermined the way users think about virtual and social networks. The poor ability of users to develop a social identity increases the chances of reluctance to use virtual networks (Krasnova et al., 2009). Enhanced user engagement in the metaverse depends on the motivational and psychological states of the virtual network users. Social factors help users to better express themselves, develop users' interaction with others, and build social identities (Dwivedi et al., 2022). The identity of people in virtual networks interacts with the way they communicate with users. Social identity refers to the way people are identified by external signs such as norms, values, customs, legal frameworks, and standards. The social identity of users is created based on social affiliation, communication, and institutional affiliation. In virtual space, users have less control due to the prevalence of anonymous identities and the lack of identity markers. Consequently, many users need to perform authentication to verify identity. Social identity in virtual networks is an important factor in reducing the risk of violating users' privacy and security (Hoang & Jung, 2015). As such, the following hypotheses are proposed:

H6a: *Social identity has a significant impact on privacy.*

H6b: *Social identity has a significant impact on security.*

3.2. Technical features effect on security and privacy

Technical features complement the social aspect by leading users to different levels of behavior in the virtual environment. Technical features (e.g., Immersive experience) are drivers of user behavior and include immersive experience and invisibility. Immersive experience provides attractive and unforgettable factors by attracting the user to an imagined world that increases the chances of interaction (Suh & Cheung, 2019). Immersive experience is a more compelling approach to different information systems. Immersive experience increases interactions between users under a high level of security and privacy. Immersive experience is the axis of cohesion for virtual networks, which are considered an information system within the various types of information systems (Schütte et al., 2022). Immersive experience is well established in information systems research, especially in understanding user behavior. The technical aspect refers to technological artifacts, which in turn increases the protection of users and provides sufficient security space. Immersive experience is a technical design that contribute to limiting user behavior in the metaverse. Thus, immersion contributes to creating an emotional and psychological feeling for users in order to increase the interaction between the bodies and senses of users and the virtual context. However, such a virtual space is affected by the privacy and security factor, which affects the perception and gestures of users (Wang et al., 2023). Virtual networks provide immersive experiences for many users, but disruptive attacks and unauthorized access can affect the functionality of the metaverse. Security and privacy attacks create multiple issues and generate confusing safety for users (Valluripally et al., 2023). Immersive experiences in virtual networks enable users to share their identity with other users. Furthermore, users feel safe and secure because immersive experiences transport the user to multiple different times, places, and viewpoints. However, immersive experiences pose a real risk to users' privacy and security because it requires a lot of sensitive data and information. For example, users may share video clips virtually, but such clips can reveal information and faces that the user does not want to share (Dwivedi et al., 2022). Therefore, we assume that:

***H7a:** Immersive experience has a significant impact on privacy.*

***H7b:** Immersive experience has a significant impact on security.*

Technical design specifies the eventual materialization of metaverse capabilities. Hence, invisibility is part of the technical design that contributes to achieving high levels of security and privacy by helping to temporarily hide the user's avatar to confuse attackers (Wang et al., 2023). Invisibility allows users to perform activities virtually invisible to others (Suh & Cheung, 2019). Overall, significant developments in virtual networks have increased users' concerns about the privacy and security of the metaverse. Problems with technical features such as invisibility increase the chances that users in virtual networks will be exposed to unhealthy behaviors such as the violation of personal information, sexual harassment, and verbal abuse (Sengupta & Cao, 2022). Due to the spread of digital and virtual technologies based on interactions that are characterized by invisibility, the possibility of maintaining the security and privacy of users has decreased significantly (Schütte et al., 2022). Threats to privacy and security have been exacerbated because users performing invisibility tasks and activities repeatedly and leave a vulnerability or digital fingerprint for attackers. Such vulnerabilities are used to collect information about users and threaten security and privacy by taking or recording photos of users. Moreover, representing users in virtual networks realistically becomes an urgent need. For example, virtual networks can be developed to be able to provide emotional interactions, reactions, and expressions with other users in virtual networks (Wang et al., 2023). Invisibility creates an inadequate context in the virtual environment and exposes users to a violation of information security and privacy through third-party access to information or financial records. In addition, invisibility can expose users to physical violations such as access to the user's body and actions. Finally, invisibility affects user interactions and relationships and can violate relational security and privacy (O'Brolcháin et al., 2016). Accordingly, we propose that:

***H8a:** Invisibility has a significant impact on privacy.*

***H8b:** Invisibility has a significant impact on security.*

3.3. The mediating effect of security and privacy

Metaverse users use various media to practice virtual activities such as mobile devices, laptops, augmented reality devices, and various internet of things devices. Using such devices, users engage in behaviors that range from positive to negative. Such a process is under the threat of an unlimited number of attackers who attack databases, devices, hardware, and networks (Dwivedi et al., 2022). In addition, metaverse services and systems are exposed to the risk of violating privacy and security. Many academics and practitioners have claimed that security and privacy play a indicating role among users' activities and online networks (e.g., Dwivedi et al., 2022; Wang et al., 2023). A huge number of people have immersed themselves in digital technologies and approximately 3.8 billion people around the world are using smartphones. Metaverse networks that possess superior privacy and security are cohesive and eternal. The privacy and security of users in the metaverse is a major concern of many academics and practitioners because the lack of security in virtual networks is considered a breach of user rights. However, little attention has been focused on the privacy and security risks in the metaverse. In addition, the increasing reporting of cases of deviant behavior in virtual networks and breaches of users' privacy and security confirms the little interest in investigating the mediation of security and privacy risks in the context of the metaverse (Dwivedi et al., 2023). Privacy and security issues in the metaverse are exacerbating by the complexity of the shape and the lack of qualified personnel to deal with privacy and security issues and to develop a secure context for the metaverse (Schütte et al., 2022). Much interest in the metaverse has been matched by little investigation into the metaverse's privacy and security issues. Security and privacy in the metaverse are essential because malicious users proliferate in virtual networks and wait for opportunities to perform real-time behaviors towards other users that violate values and norms (Dwivedi et al., 2022). Privacy and security issues in the metaverse keep moving forward nonstop. The metaverse is characterized by newness and complexity, which in turn makes it difficult to detect deviant attacks and practices on such platforms, especially since the metaverse has no limits (Alspach, 2022).

According to Falchuk et al. (2018), the use of private copy would affect the psychological motivations of users by creating a temporary copy for users that provides sufficient protection for the user from attacks and deviant behaviors by other users. Once privacy and security precautions are in place, users can utilize metaverse services without worrying about deviant behavior. Adequate security measures must be available in the metaverse to protect the privacy and security of users from various threats (Zhang et al., 2022). The metaverse collects sensitive information about users, for example, conversations and videos can be recorded, and eye technology can record user usage. Several measures have been proposed to avoid privacy and security issues by providing two-factor authentication and using encryption (Dwivedi et al., 2022). Some users use the metaverse for malicious purposes due to the lack of privacy and security, which raises concerns among users about exposure to many harms in virtual reality. Social and technical influences play a major role in managing privacy and security. The harmful behavior of users in the metaverse has gone beyond criminality (Gao et al., 2023). Managing security and privacy in the context of the metaverse is indispensable. Several solutions have been proposed, for example security by design is a cybersecurity approach to formalize the metaverse to increase the security of virtual networks and rein in malicious users. All privacy and security measures shall be included in all phases of maintenance and development of the metaverse to avoid practicing deviant behaviors and create a safe and sound virtual context for users (Dwivedi et al., 2022). The infrastructure of virtual systems such as the metaverse constitutes strength and ensures reliability and trustworthiness of use. The intense and excessive use of Internet networks makes virtual platforms more difficult for users. Defects in the technical and social aspects weaken the wall of security and privacy and provide the basis for launching attacks and practicing deviant behaviour. Studying the security and privacy problem of virtual networks as a sociotechnical problem reveals the nuanced interactions between virtual systems and users. The socio-technical problem requires understanding the interaction and psychology of users with digital and virtual platforms (Alspach, 2022). The mediation of security and privacy between sociotechnical aspects and user behavior in virtual networks has recently attracted the attention of information systems scholars. But few studies have investigated such a relationship (Bella et al., 2015). Therefore, this study assumes the following:

> ***H9:*** *Privacy and security have significant impact on deviant behaviors in the metaverse.*
>
> ***H10:*** *Privacy and security mediate the relationship between social, technical features, and deviant behaviors in the metaverse.*

4. Methodology

4.1. Sample

The target population for this study is users of virtual networking sites such as Sandbox, Decentraland, and Axie Infinity. Credamo was used to collect data for this study. Credamo is a popular online data collection platform for behavioral studies (Fute et al., 2022). The link to the online survey for the period December 2022-July 2023 was shared. To ensure that the target sample are users of metaverse platforms, the current study used a filtering question that includes "Have you ever used the metaverse?" If the answer is yes, please continue completing the questionnaire. Otherwise, please stop. Credamo offers paid massive data collection services. Previous literature recommended relying on the Credamo platform to collect data. Therefore, the platform assumed access to many metaverse users. Moreover, this study used a non-probability sampling method because the authors did not have a list of metaverse users. According to Hair et al. (2011) the sample size should be ten times larger or equal to the formal indicators or larger than the number of structural paths. In order to address the common bias issue, the questionnaire was distributed over three times. The first time included the questionnaire about the independent variables, which are the technical and social elements, and the number of respondents was 2313. In the second round, the same respondents were asked about the mediate variables (i.e., Security and privacy) and we received 1672 responses. Finally, the third round included the question about the dependent variable, and the number of respondents reached 1121. Therefore, the remaining 1121 valid responses were involved in the ultimate dataset. We make sure respondents have experience in the metaverse. Otherwise, it will abort on the first page. A 5-point Likert scale was used based on previous studies. The measurement tool was presented to six experts in the information system, and slight modifications were made to the scale. Table 1 shows demographics of respondents.

4.2. Analytical approaches

Bias and variance are a focus of suspicion in social science studies. Common bias method has become a concern in much research. There are two approaches to addressing such anxiety: procedural and statistical. In terms of procedural, our study benefited from distributing the questionnaire on the basis of three times to reduce bias in the data. Different cover stories were used for all scales to increase psychological separation. In the context of statistical methods, Harman's single-factor analysis was performed and the variance for the first factor was 32.35, which is less than the recommended variance of 50% (Podsakoff et al., 2003). Similar to previous literature such as Lin et al. (2015) and Wolter and Cronin (2017), Marker Variable has been adopted. This study measured this variable by adopting attitudes towards private label brands, which included five

Table 1. Demographics of respondents.

Demographics	Categories	Frequency	Percent (%)
Gender	Male	753	67
	Female	368	33
Age	18–24 years	245	22
	25–34 years	339	30
	45–54 years	492	44
	Over 55 years	45	4
Virtual Networking Sites	Sandbox	371	33
	Decentraland	389	35
	Axie Infinity	361	32
Education Qualification	Diploma	371	33
	Bachelor	462	41
	Master	137	12
	Doctoral	51	5
Employment Status	Working (Salaried)	469	42
	Working (Self-employed)	374	33
	Not Working	278	25
Country	USA	476	42
	China	371	33
	Other Countries	274	24

items (e.g., Buying private label brands makes me feel good) (Burton et al., 1998). Marker Variable has been added to the structural path and linked with dependent variable and R^2 calculation before and after adding this variable. R^2 values show slight differences before and after link Marker Variable with dependent variable. Therefore, common method variance/bias is not a concern for the current study. The data of the study were subjected to normal analysis and collinearity testing. The normal distribution test confirms that there is no concern in this regard. Also, Collinearity Testing reports that the correlations between the variables were less than 0.9. Therefore, there is no interpretational and methodological problem because of multicollinearity, and there is no need to remove one or more variables from the conceptual framework.

5. Results

5.1. Partial least squares based structural equation modeling

PLS-SEM analysis has become widely recommended by social science scholars. Second generation analysis (i.e., PLS-SEM) captures causal relationships and tests theory. To proceed with the analysis of causal relationships, convergent and discriminant validity must be tested. To evaluate convergent validity the average variance extracted (AVE), composite reliability (CR), and loading factor (LF) should be tested (Al-Abrrow et al., 2023; Khaw et al., 2023). Findings shown in Table 2 reveal that the values are consistent with the established parameters of the PLS-SEM method. The values of CR and LF met the criteria of the PLS-SEM method and for all variables were greater than 0.7. In addition, the AVE values met the specified criteria and were greater than 0.5.

The results of the model evaluation revealed that the concern in convergent validity vanished because all values met the evaluation criteria with the deletion of items that have LF less than 0.7. But the discriminant validity needs to be further explored. For this end, the heterotrait-monotrait ratio of correlations (HTMT) method is illustrated in Table 3.

The HTMT test met the recommended model evaluation criteria and the results revealed acceptable discriminatory validity. To capture the causal relationships and test the theory on the study sample, the evaluation of the structural model was used. To capture the causal relationships and test the theory on the study sample, the evaluation of the structural model was used. This study employed bootstrapping with 5000 subsamples for path estimates. Table 4 illustrated hypotheses tested.

In terms of significance, the results confirm the relationships for all paths are supported except self-efficacy and personal traits. The social and technical perspective is crucial in controlling deviant behaviors in the virtual world. In addition, the aspect of privacy and security hold back from exacerbating the negatives side of metaverse.

5.2. Fuzzy set qualitative comparative analysis

The PLS-SEM method captures the causal and indirect relationships between the constructs. This study investigates the sociotechnical approach theory on a sample of users of virtual reality platforms in different countries. To this end, the second-generation approach (PLS-SEM) is more ingenious and justifiable for testing the theory used. However, previous literature raised a number of concerns associated with the adoption of such a method. For example, previous studies raised the issue of not capturing nonlinear relationships and handle a small number of cases. Nonlinear issues have been addressed by incorporating an artificial neural network (ANN) approach to reveal non-compensatory and non-linear relationships between constructs (Alnoor et al., 2022). However, the literature has criticized the combination of ANN with PLS-SEM method because there are selection problems within the architecture for the implementation of the ANN analysis (Zaidan et al., 2023). The fsQCA approach is interesting and addresses the problem of PLS-SEM by mitigating the small sample problem and maximizing the number of comparisons to the data under analysis. Such an analysis supports rate unclassifiable items easily. The fsQCA analysis is a link between quantitative and qualitative methods. Also, fsQCA analysis calculates the net effect of variables. Such an approach focuses on asymmetric relations between the antecedent and the result. For example, control variables may be part of the solution. This analysis contributes to providing multiple solutions due to insufficient regression analysis to provide comprehensive solutions. The fsQCA analysis is useful for different types of data, including the five-point Likert scale. Utilizing fsQCA software to perform formative modeling and quantitative comparative analysis. The fsQCA analysis includes three stages: data calibration, necessary condition analysis, and truth table analysis. In the data calibration stage, the raw data is transformed into standard values by converting Likert scale numbers (In this study the five-point scale was used) into fuzzy values ranging from 0 to 1. Zero indicates absence of membership, 1 indicates full membership, and 0.5 indicates crossover point. The truth table presents a number of criteria which represent k and 2^k represent rows. The truth table supports the results to be more rigorous. It is determined whether the group interprets the result or not. Using consistency thresholds, the author inserts a value of zero or one for the column with the output variable. The final stage includes solutions to obtain possible configurations (Pappas & Woodside, 2021). In the necessary conditions test, it is determined whether the effect for each condition is necessary for the outcome. The consistency value must be less than 0.90 to determine if the condition is necessary (Ali et al., 2023).

The fsQCA analysis uses many types of data. Therefore, data calibration is one of the critical steps in such an analysis. The study variables must be calibrated and converted into a fuzzy environment ranging from 0 to 1. One indicates full membership, zero indicates full non-membership, and 0.5 is considered intermediate set. Each level of membership is defined fully in, intermediate, and fully out. In the current

Table 2. Measurement model (LF, AVE and CR).

Constructs	Adapted items	FL	CR	AVE	Source
User-to- user interaction	Interact with the virtual network to search for information	0.778	0.869	0.624	Onofrei et al. (2022)
	Interact with the virtual network to read other users' tips and experiences	0.839			
	I interact with the virtual network to read reviews of other users	0.791			
	I interact with the virtual network to read other users' recommendations	0.748			
Homophily	People in the virtual network have similar likes/dislikes like I do	0.789	0.878	0.643	Onofrei et al. (2022)
	People in the virtual network have the same values as I do	0.827			
	People in the virtual network have the same experiences as I do	0.841			
	People in the virtual network have the same preferences as I do	0.748			
Personal traits	I see myself as warm	0.653	0.900	0.601	Khedhaouria and Cucchi (2019)
	I see myself as sympathetic	0.747			
	I see myself as kind	0.780			
	I see myself as imaginative	0.624			
	I see myself as creative	0.807			
	I see myself as extraverted	0.801			
	I see myself as talkative	0.758			
	I see myself as anxious	0.525			
	I see myself as moody	0.559			
	I see myself as easily upset	0.614			
	I see myself as organized	0.591			
	I see myself as self-disciplined	0.502			
Self- efficacy	I can use this virtual network if I see someone else using it	0.791	0.842	0.641	Sharma et al. (2022)
	This virtual network can be used if someone else helps get started	0.721			
	I can use this virtual network if someone shows me how to use it first	0.881			
Social identity	I consider all virtual network users to be the same group	0.839	0.905	0.704	Shih and Huang (2014)
	I have a strong inclination to become a member of the virtual network	0.868			
	There is a strong connection between me and other users of the virtual network	0.836			
	I don't feel any boundaries between myself and other users in the virtual network	0.813			
Social ties	I meet my friends as often as I want in the virtual network	0.817	0.864	0.680	Lee et al. (2019)
	I spend enough time with my family or friends over the virtual network	0.857			
	I have a lot of opportunities to talk to others in the virtual network	0.798			
Immersive experience	The metaverse created a new environment that suddenly disappeared at the end of the show	0.744	0.909	0.667	Jafar and Ahmad (2023)
	Sometimes, I wasn't aware of my surroundings	0.808			
	I'm immersed in what I'm doing on metaverse	0.857			
	I lost track of the reality of the outside world through metaverse use	0.847			
	My focus doesn't stray when I'm on the metaverse	0.823			
Invisibility	I feel that my presence in virtual networks matters	0.728	0.886	0.610	Batool and Kashif (2023)
	I feel that users in virtual networks are listening to me carefully	0.792			
	I feel like users mistreat me in virtual networks	0.825			
	I feel like users in virtual networks are keeping me at a distance	0.825			
	I feel like users in virtual networks are making fun of me which makes me think I'm not human	0.728			
Privacy risks	I am sensitive about providing information about my preferences	0.845	0.909	0.713	Ameen et al. (2022)
	I am concerned about information being collected while using virtual networks	0.890			
	I am concerned about the use of my personal information in virtual networks	0.844			
	I am concerned about how my personal information will be used in virtual networks	0.798			
Security risks	I am confident that information that I provide while using virtual networks will only reach their system	0.707	0.851	0.589	Balapour et al. (2020)
	I believe that third parties may deliberately access information while using virtual networks	0.779			
	I believe that the information I provide while using virtual networks will not be tampered with	0.808			
	I have confidence in the safety of using virtual networks	0.771			
Deviant behaviors in the metaverse	I am looking for another user on the virtual network to talk to about sex or have sex with	0.840	0.885	0.719	Kabiri et al. (2021)

(*continued*)

Table 2. Continued.

Constructs	Adapted items	FL	CR	AVE	Source
	I am sending a partly naked photo or video to another user on a virtual network	0.856			
	I make rude or vulgar comments over virtual networks	0.847			
	I harass or embarrass other users on virtual networks	0.625			
	I spread rumors about a user whether it is real or not on virtual networks	0.619			
	I went to pages to intentionally display sexual material	0.572			
	I am trying to hack another user account on virtual networks	0.664			

Table 3. Discriminant validity (HTMT).

Variables	1	2	3	4	5	6	7	8	9	10	11
1. Deviant behaviors in	▨										
2. Homophily	0.563	▨									
3. Immersive experience	0.784	0.589	▨								
4. Invisibility	0.664	0.592	0.764	▨							
5. Personal traits	0.698	0.815	0.691	0.634	▨						
6. Privacy risks	0.558	0.391	0.776	0.764	0.499	▨					
7. Security risks	0.836	0.490	0.762	0.748	0.596	0.744	▨				
8. Self-efficacy	0.610	0.661	0.731	0.739	0.685	0.709	0.632	▨			
9. Social identity	0.660	0.636	0.772	0.742	0.712	0.833	0.747	0.712	▨		
10. Social ties	0.767	0.649	0.738	0.745	0.742	0.732	0.704	0.780	0.796	▨	
11. User interaction	0.662	0.810	0.591	0.517	0.740	0.359	0.522	0.611	0.582	0.612	▨

study, data calibration was performed directly by the authors because this method was recommended by the previous literature on fsQCA to use it to give rigorous results. To perform a data calibration, breakpoints must be defined, and they must not be zero and one, because this will give positive and negative infinity. Previous literature advises utilizing from the use of percentiles. Ratios such as 95%, 50%, and 5% can be used as thresholds in fsQCA, especially since the data of our study is normally distributed and we used the five-point Likert scale. Such values provide an accurate representation of our sample. In addition, for data calibration purposes, the data is cut into quintiles. Cross-tabulations were employed between quintiles, and the results showed that there is heterogeneity that the main effect cannot adequately capture and describe (Pappas & Woodside, 2021). Necessary condition analysis (NCA) was performed to identify the contributing and essential factors to deviant user behavior in virtual networks (see Table 5). The condition is necessary when consistency and coverage values are greater than 0.9 and 0.5, respectively.

Table 5 shows that engaging in deviant behavior in virtual networks requires the presence of user-to-user interaction (Consistency = 0.985, Coverage = 0.750), social identity (Consistency = 0.922, Coverage = 0.849), social ties (Consistency = 0.991, Coverage = 0.810), invisibility (Consistency = 0.914, Coverage = 0.753), privacy risks (Consistency = 0.900, Coverage = 0.722), and security risks (Consistency = 0.921, Coverage = 0.844). The results reveal that the aforementioned prerequisites are necessary to mitigate deviant user behavior in virtual networks. The sufficient condition analysis was used to discover the extent to which the virtual network users' data provided a sufficient explanation for the expected results. Table 6 presents configurations sufficient to predict the deviant behavior of users of virtual networks. The solutions were accepted because the values of consistency and coverage were greater than 0.2 and 0.8, respectively.

As mentioned earlier, there are three types of solutions, namely complex solution, parsimonious solution, and intermediate solution. Previous literature recommends the use of an intermediate solution because it provides stringent results. Also, intermediate solution includes peripheral and core conditions. Therefore, peripheral and core elements must be determined for each configuration in order to deeply understand the deviant behavior of virtual network users. Table 6 shows that the absence of the condition is represented by a circle drawn with a cross (⊗). The black circle (●) indicates the presence of the condition. Empty spaces represent unimportant solutions. In addition, the large black circle represents core conditions, while the small black circle represents peripheral conditions. The results in Table 6 show that the overall coverage and consistency were 0.819 and 0.928, respectively. The results reveal that the seven solutions cover a large percentage of the outcome. To reduce deviant behavior in virtual metaverse networks, the fsQCA results approach seven core solutions. The first, second, third, and fourth solutions highlight that user-to-user interaction, homophily, personal traits are among the core and important constructs. The combination of user-to-user interaction, homophily, personal traits, and self-efficacy leads to low levels of deviant behavior in virtual networks with the absence of social ties, immersive experience, and privacy risks (3 solution). Or a combination of social ties, immersive experience, invisibility, privacy risks, and security risks (Solutions 5 and 7). To this end, user to user interaction, homophily, personal traits, social ties, immersive experience, invisibility with the absence of privacy risks are critical factors in reducing deviant behavior in virtual networks (Solutions 6). The fsQCA results showed all possible solutions, and in order to test the validity of the proposals and the linkage of the information in the sample, specific

Table 4. Hypotheses test.

Direct path	Beta	Sig	P	Result
User to user interaction -> Privacy risks	0.060	2.206	0.027	Yes
User to user interaction -> Security risks	0.082	2.549	0.011	Yes
Personal traits -> Privacy risks	0.005	0.175	0.861	**No**
Personal traits -> Security risks	0.051	1.329	0.184	**No**
Self-efficacy -> Privacy risks	0.045	1.680	0.093	**No**
Self-efficacy -> Security risks	0.048	1.378	0.168	**No**
Social identity -> Privacy risks	0.470	13.754	0.000	Yes
Social identity -> Security risks	0.155	4.169	0.000	Yes
Social ties -> Privacy risks	0.051	2.564	0.000	Yes
Social ties -> Security risks	0.436	10.379	0.000	Yes
Homophily -> Privacy risks	0.146	4.872	0.000	Yes
Homophily -> Security risks	0.100	3.165	0.002	Yes
Immersive experience -> Privacy risks	0.072	2.590	0.000	Yes
Immersive experience -> Security risks	0.050	2.063	0.000	Yes
Invisibility -> Privacy risks	0.502	12.363	0.000	Yes
Invisibility -> Security risks	0.172	3.865	0.000	Yes
Privacy risks -> Deviant behaviors	0.112	3.667	0.000	Yes
Security risks -> Deviant behaviors	0.602	21.986	0.000	Yes
Indirect paths				
User to user interaction -> Privacy risks -> Deviant behaviors	0.107	3.880	0.000	Yes
User to user interaction -> Security risks -> Deviant behaviors	0.050	2.508	0.012	Yes
Personal traits -> Privacy risks -> Deviant behaviors	0.001	0.167	0.868	**No**
Personal traits -> Security risks -> Deviant behaviors	0.031	1.311	0.190	**No**
Self-efficacy -> Privacy risks -> Deviant behaviors	0.005	1.552	0.121	**No**
Self-efficacy -> Security risks -> Deviant behaviors	0.029	1.383	0.167	**No**
Social identity -> Privacy risks -> Deviant behaviors	0.053	3.540	0.000	Yes
Social identity -> Security risks -> Deviant behaviors	0.093	4.071	0.000	Yes
Social ties -> Privacy risks -> Deviant behaviors	0.106	3.391	0.000	Yes
Social ties -> Security risks -> Deviant behaviors	0.263	9.393	0.000	Yes
Homophily -> Privacy risks -> Deviant behaviors	0.016	3.146	0.002	Yes
Homophily -> Security risks -> Deviant behaviors	0.060	3.120	0.002	Yes
Immersive experience -> Privacy risks -> Deviant behaviors	0.108	4.342	0.000	Yes
Immersive experience -> Security risks -> Deviant behaviors	0.130	3.055	0.000	Yes
Invisibility -> Privacy risks -> Deviant behaviors	0.056	3.647	0.000	Yes
Invisibility -> Security risks -> Deviant behaviors	0.104	3.944	0.000	Yes

Table 5. Necessary condition analysis.

Conditions Tested	Consistency	Coverage
UTU	**0.985**	**0.750**
∼UTU	0.518	0.669
HOM	0.648	0.854
∼HOM	0.482	0.661
PAT	0.592	0.896
∼PAT	0.551	0.666
SFE	0.564	0.828
∼SFE	0.567	0.702
SOI	**0.922**	**0.849**
∼SOI	0.492	0.651
SOT	**0.991**	**0.810**
∼SOT	0.507	0.667
IME	0.579	0.761
∼IME	0.503	0.692
IVS	**0.914**	**0.753**
∼IVS	0.493	0.731
PRR	**0.900**	**0.722**
∼PRR	0.486	0.738
SUR	**0.921**	**0.844**
∼SUR	0.494	0.656

Note: UTU = User-to- user interaction, HOM = Homophily, PAT = Personal traits, SFE = Self- efficacy, SOI = Social identity, SOT = Social ties, IME = Immersive experience, INS = Invisibility, PRR = Privacy risks, SUR = Security risks.

configuration in fsQCA was calculated and drawn as shown in Figure 4.

The consistency value was 0.924 for specific propositions. For testing specific propositions, function (fuzzyand x,.,) was adopted, where all variables were taken into account. In addition, the negation of a specific condition was tested by employing the fuzzynot(x) function for every variable that is negated. Then the fyzzyand function was executed, which took all the variables in the configuration model with the new variable extracted from the fuzzynot(x) function. The new variable (model) has been drawn as shown in Figure 5.

The consistency value for model 1 was 0.952. The results confirm that the consistency values were greater than 0.80 and this is considered as a solid preamble to theory advancement. The results of the current research also provide partially support to the proposition. Hence, high scores in the proposed configurations occur for low scores of deviant behaviors by users in virtual networks. Predictive validity testing of solutions should be performed. The predictive validity procedure offers the possibility of the model succeeding in predicting the result in additional samples. According to Pappas and Woodside (2021), the sample was divided randomly into two parts, namely the subsample and holdout sample, and the same analysis was conducted for the two samples. The results were obtained for the subsample. The holdout sample was then used to test predictive validity. The fuzzyand(x, … ,) and fuzzynot(x) functions were used to obtain the graph. The results reveal that the consistency values for the two samples were 0.927, 0.910, respectively, and the coverage were 0.779, 0.812, respectively. Thus, there are no significant differences between the two samples, and this confirms the predictive validity of the results.

6. Discussion

Recent years have witnessed tremendous progress in the use of virtual networks, with a dangerous precedent in increasing the practice of a mixture of positive and deviant behaviors by users. Understanding the user engagement and deviant behaviors of the metaverse alleviates the dark side of such technologies and contributes to enhancing the bright side of using virtual networks in business models. Previous literature had an influential imprint in identifying the essential antecedents for the practice of deviant behaviors such as social and technical factors. The literature has argued that investigating of factors such as user-to-user interaction, homophily, personal traits, self-efficacy, social identity, social ties, immersive experience, and invisibility hold back the deviant behavior of users of virtual metaverse networks. As such, a sociotechnical perspective was relied upon because understanding the behavioral perspective of the metaverse phenomenon is of particular importance to the information systems literature to understand how deviant behaviors are practiced by users and to investigate issues arising from such phenomena. Data collected from users in the United States, China, and several other countries show that user-to-user interaction, homophily, social identity, social ties, immersive experience, and invisibility suppress deviant user behavior in social networks. However, the results revealed that technical and social factors cannot mitigate the dark side of users in virtual networks without considering privacy and security aspects. Previous literature arguments confirm these findings regarding the role of technical and social features in addition to privacy and security risks in encouraging deviant behaviors in the metaverse (e.g., Dwivedi et al., 2022).

Table 6. FsQCA findings.

	Solution						
Conditions	1	2	3	4	5	6	7
User to user interaction	●	●	●	●	⊗	●	
Homophily	●	●		●	●	●	●
Personal traits	●	●	●	⊗		●	●
Self-efficacy	●		⊗		●		
Social identity		●					
Social ties	●	●	⊗		●	●	●
Immersive experience		●	⊗	●	●	●	●
Invisibility					●	●	●
Privacy risks			⊗	●	●	⊗	●
Security risks	●	●	⊗	●			●
Raw Coverage	0.448	0.471	0.304	0.297	0.281	0.240	0.450
Unique Coverage	0.010	0.009	0.006	0.005	0.006	0.002	0.005
Consistency	0.922	0.916	0.845	0.874	0.854	0.923	0.883
Overall Coverage	0.819						
Overall Consistency	0.928						

The originality and merit of this study is that it provides a deep understanding of the mechanisms and configurations that encourage deviant behaviors in the metaverse. We provide additional insights into deviant user behaviors from the sociotechnical perspective in the metaverse. The study aims to inform practitioners and academics of information systems and the virtual reality business industry about enhancing the bright side of the metaverse phenomenon by delivering signals in a timely manner in response to protecting users from deviant behaviors in virtual reality and

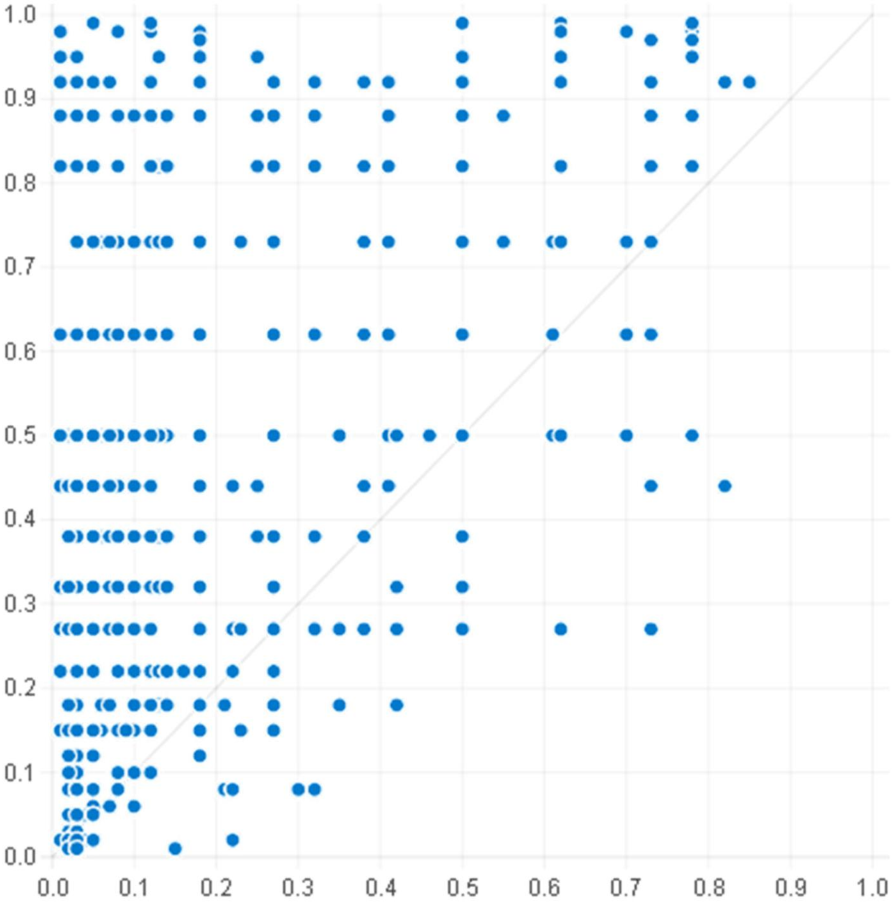

Figure 4. Plotting a specific proposition.

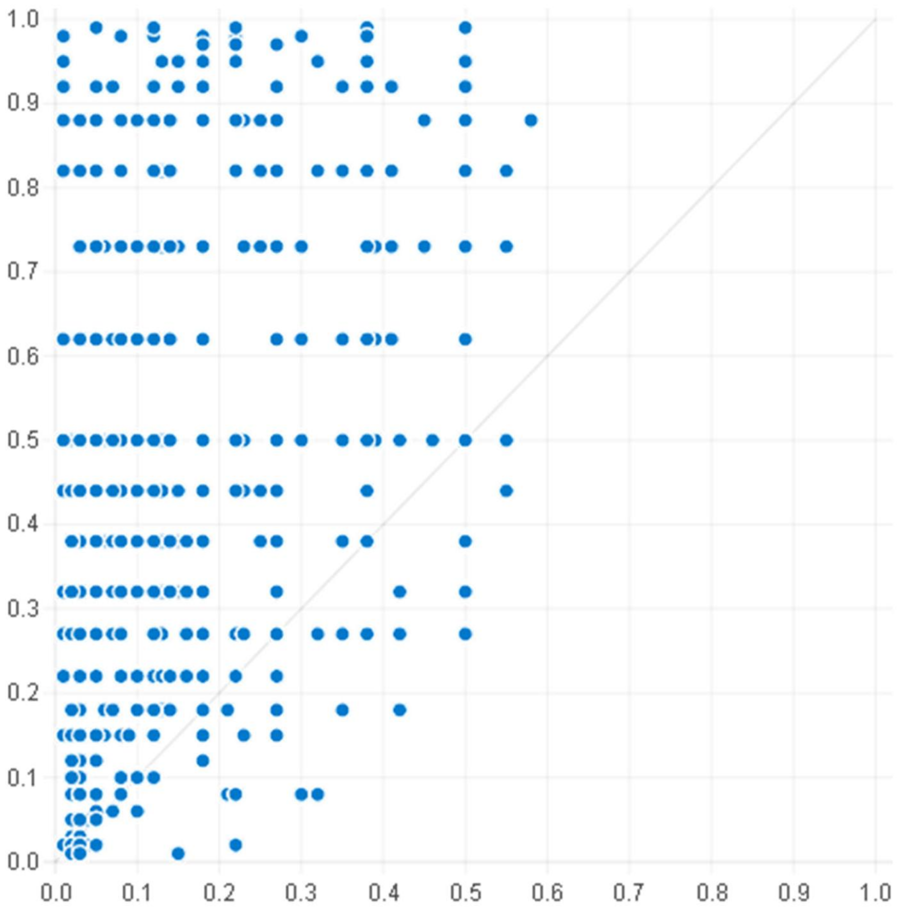

Figure 5. Fuzzy plot of model 1.

reducing victims of online malpractices resulting from users' feeling of comfort due to online disinhibition. Online disinhibition is an important driver of deviant behavior online. Because online disinhibition is a psychological state that makes users feel relaxed and engage in more daring behaviors in virtual reality.

Contrary to expectations, the effect of personal traits and self-efficacy on deviant behavior of users in virtual networks is not significant. Virtuous personality traits are more relevant to reality than to virtual reality (Abdullah & Marican, 2016; Zhang & Zhao, 2022). Therefore, online disinhibition prevails over the virtuous personal traits in the virtual networks and the personality traits cannot be a protective factor. The deviant behavior of users in virtual networks is not linearly related to self-efficacy. Because deviant behavior in virtual reality is affected more by peer pressure. While the interaction between the users and the deviant behavior of the users is significant because the deviation of the users is contagious. In virtual networks, users are usually together during virtual reality experiences. Interactions between users create an environment in which independent decision making is difficult to achieve and interactions affect others. Escalating behavior in virtual reality is a contagious epidemic that spreads among users at breakneck speeds and angers users. A significant relationship was found between homophily and deviant user behavior in virtual networks because users in the virtual context usually bond with similar others. In terms of social identity and social ties, engaging in deviant behavior in virtual networks is less when users are primed with a broad social identity. Social identity and social ties support the development of a higher awareness of behavioral deviance towards other users in virtual networks. Identity and social ties are a vital driver of users' actions. Preparing a broad social identity would mitigate deviant and abnormal behaviors in virtual networks, which reinforces the social identity theory.

The results revealed that the technical factors represented by immersive experience and invisibility have a role in reducing deviant behaviors in the virtual reality context. For example, immersive merchants such as having cut down a virtual tree triggers a burning desire to preserve the environment. Thus, with regard to deviant behavior, virtual networks can be developed such as designing games aimed at protecting users from abnormal and deviant behavior by giving players a distinctive card that can be shared with colleagues. The same goes for invisibility, which is associated with reported threats in virtual networks. Enforcing invisibility increases users' engaging in lewd and deviant behavior of virtual reality. These results are in line with previous literature (e.g., Lapidot-Lefler & Barak, 2012) that indicated that anonymity and poor invisibility increase the practice of toxic behaviors online. One of the explanations for such results is that anonymity increases the chances of being found under pseudonyms. For example, in paper dealings, the pseudonym is an important factor in anonymity, while in face-to-face meetings, the name is not necessary for identification. Invisibility an intrinsic factor for increasing disinhibiting behaviors in virtual networks. Metaverse provides incredible services in various fields such as education, health, tourism and business. Nevertheless, the results of this study raised decisive results regarding the vulnerability of virtual networks to security and privacy risks. The leakage of user data and the presence of many users who use pseudonyms in metaverse networks, as the privacy and security of users is under constant threat from malicious parties. Security and privacy in the metaverse are critical issues for maximizing the benefits of virtual networks. Malicious users engage in behaviors that violate human values. Therefore, providing users with effective security and privacy services ensures that users are protected from threats and toxic practices. This study responds to recent calls to pay more attention to the concept of deviant work behavior in virtual networks (Dwivedi et al., 2022). The current study advances many speculations to theories and industry by investigating deviant behavior by metaverse users because existing studies provide inconclusive results for users to engage in toxic behaviors in virtual networks. The proposed model contributes to the limited literature on deviant behavior across virtual networks. By investigating the sociotechnical approach and the presence of privacy and security factors, we seek to provide critical implications for academics and policymakers.

6.1. Theoretical implications

Theoretically, the use of a hybrid approach that includes the PLS-SEM input and the fsQCA introduce a new approach for information systems researchers compared to previous studies that relied only on the net effect approach. Capturing causal and linear relationships and testing the measurement model (validity and reliability of the model) is done via PLS-SEM analysis. The fsQCA approach complements the work of the PLS-SEM analysis and identifies sufficient causal configurations (combining factors together) to mitigate deviant user behavior in virtual networks. Seven core solutions have been found to address deviant user behavior in the metaverse utilizing fsQCA. The presented solutions are considered substantial because they have developed a socio-technical perspective and opened up important prospects for academics in the field of information systems in order to create a friendly and useful virtual reality. Compared with previous literature, such as Zhou et al. (2022), which investigated deviant disclosure behavior on internet platforms using neutralization theory. The current study attempted to investigate the deviant behavior of users from a sociotechnical perspective. Thus, this study is considered one of the few studies that investigated the deviant behavior of users in virtual networks. The current study distinguishes itself by advancing technical and social theory and providing more ultimate findings regarding the metaverse's dark side. To the best of our knowledge, this study is the first to respond to the call of previous literature (Dwivedi et al., 2022; Singla et al., 2022) on the need to study the impact of technical and social factors, privacy and security factors to detect and limit deviant behavior of users through virtual networks. Although previous literature (e.g., Zhang et al., 2022) has revealed concerns about privacy and security in virtual networks, little attention has been paid to investigating deviant user behavior from a sociotechnical perspective. This study opens a new avenue for academics to improve the vulnerabilities of information systems related to the detection of unhealthy information, fraud, plagiarism, etc. by providing our experimental results with additional understanding of deviant behavior in the metaverse.

6.2. Practical implications

Managerially, the findings of this study provide insights and guidance for managers of information systems companies to develop a more harmonious virtual context. The metaverse can become an immersive experience and create new and vast social interactions. Metaverse adoption has changed the behavior of many people. Practitioners should encourage interaction between users, create different links between them, introduce techniques such as virtual games based on interaction, and establish strong links and bonds between users to avoid obscene behaviors. We advise practitioners and policymakers to hold training and educational workshops on the use of virtual networks in order to convince users not to harm others. Virtual platforms should seek to put in place effective policies and procedures to protect users from deviant behaviors such as sexual harassment or verbal abuse, etc. to mitigate the risk of misuse. Deep algorithms that reveal user information can also be used by relevant government agencies to address and mitigate the practice of deviant behavior in the metaverse. Information systems practitioners can monitor user trends in virtual networks to understand lifestyles, values, opinions, and trends to create campaigns that motivate users with similar values and attitudes to engage in the use of virtual reality services and reduce the practice of deviant behaviors. Policymakers must pay more attention to the education and development of metaverse users to increase virtuous personality traits and prevent deviant behavior across virtual networks. In addition, enhancing deindividuation cues in virtual networks may reduce deviant behavior. To activate social identity and ties, practitioners can engage in a number of activities, including sending welcome messages to users related to identity, designing interactive virtual games that focus on identity, and providing prominent identity signs. Users in the metaverse feel more connected, which increases awareness and reduces deviant behavior. In addition, practitioners can direct users that their misconduct increases the chances of obtaining a negative evaluation, which in the future leads to blocking the user's account for a period of time or providing statistics about the countries that practice the most deviant behavior in virtual networks. Thus, such an action brings a sense of shame to the comrades of the group or the country, which increases the chances of avoiding obscene and toxic behaviors. Developers of information systems can use other measures, for example, asking users to sign a pledge not to practice or engage in deviant behavior. Developing mechanisms to detect and reduce deviation in virtual networks is a recommendation for designers of information systems, which makes experiences more immersive and exciting. For example, developers and designers in the metaverse can gain an early understanding of toxic behaviors to limit and block them in such virtual networks. As we mentioned earlier, feeling relaxed is a key factor in practicing deviant behaviors online. Virtual network designers can assess online disinhibition among users to combat deviant behavior on virtual platforms.

7. Conclusion

This study makes a significant theoretical contribution by adopting a socio-technical perspective, considering both social and technical factors. It advances existing literature by exploring the impact of privacy and security factors alongside social and technical elements on deviant user behavior in the metaverse users. Hence, we seek to employ a hybrid approach, integrating PLS-SEM and fsQCA. This combination allows for a comprehensive analysis of both causal relationships and sufficient causal configurations, providing a nuanced understanding of the factors influencing deviant behaviors in virtual networks. The current study offers actionable insights to information systems companies, suggesting strategies to create a more harmonious virtual context and mitigate deviant behaviors. The recommendations cover training workshops, policy development, and the use of deep algorithms for user protection. Overall, designers and developers of virtual networks should consider different situations to enhance the metaverse context by designing configurations that are compatible with users and businesses and ignore configurations that undermine positive behavior in virtual networks. Moreover, the proposed configurational approach and the presented solutions are more feasible because it provides an insight for information systems developers to create virtual networks with high security and privacy. Accordingly, there must be authentication to access the data and store the data securely through encryption to increase the privacy and security of the data. There should also be an interest in software, hardware, and network security for the metaverse due to the presence of many malware and security threats that increase users' exposure to pornography, violence, and terrorist attacks via the Internet. It is important to consider security by design architecture because it is necessary in the early stages of designing information systems. In addition, concern for the security of devices is a critical factor in reducing the risks of privacy and security breaches, which are toxic behaviors. Therefore, securing the devices in virtual networks by adopting strict and efficient security measures and using secure chips instead of the programs on the devices contributes to increasing security and privacy, which is reflected positively in reducing deviant behaviors.

8. Avenues for future research

Like any previous and ongoing study, the current study has several constraints that are considered avenues for future research. Firstly, the study acknowledges the limitations of its cross-sectional approach. A more in-depth exploration and understanding of deviant behaviors could be achieved through a longitudinal approach, providing insights into the evolution of such behaviors over time and enabling the identification of potential causal relationships. Secondly, while the paper mentions the factors of neutralization theory briefly, there is an opportunity for a more in-depth exploration. A deeper analysis of factors such as injury, responsibility, defense of necessity, metaphor of the ledger, and avoidance of greater harm could enhance the study's theoretical framework. Thirdly, the study focuses on social and technical factors but could benefit from exploring the impact of content characteristics on deviant behavior. Factors such as information vividness, customization, and prior commitment length, as well as individual factors like self-esteem and self-regulation, could be considered for a more comprehensive understanding. Fourthly, the current study used a hybrid statistical approach by integrating PLS-SEM with fsQCA to provide solutions and configurations in order to detect and treat deviant behaviors in virtual networks. The use of statistical approaches such as multi-criteria decision-making would provide a classification of practitioners about the most and least users of deviant behavior, providing insights for practitioners to engage with good users as a model and disseminate their immersive experiences to motivate others to do the same.

Compliance with ethical standards

The author certifies that he has no other potential conflicts of interest. The research involved human participants. The survey shared with the participants explained the purpose of the research, and the data collected. Participants took part voluntarily and were given the option to skip the survey at any stage. Further, informed consent was obtained from all subjects and/or their legal guardian(s).

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

Abbas, S., Alnoor, A., Yin, T. S., Sadaa, A. M., Muhsen, Y. R., Khaw, K. W., & Ganesan, Y. (2023). Antecedents of trustworthiness of social commerce platforms: A case of rural communities using multi group SEM & MCDM methods. *Electronic Commerce Research and Applications*, *62*(11), 101322. https://doi.org/10.1016/j.elerap.2023.101322

Abbasi, G. A., Sandran, T., Ganesan, Y., & Iranmanesh, M. (2022). Go cashless! Determinants of continuance intention to use E-wallet apps: A hybrid approach using PLS-SEM and fsQCA. *Technology in Society*, *68*(2), 101937. https://doi.org/10.1016/j.techsoc.2022.101937

Abdullah, H. O., Atshan, N., Al-Abrrow, H., Alnoor, A., Valeri, M., & Erkol Bayram, G. (2023). Leadership styles and sustainable organizational energy in family business: Modeling non-compensatory and nonlinear relationships. *Journal of Family Business Management*, *13*(4), 1104–1131. https://doi.org/10.1108/JFBM-09-2022-0113

Abdullah, A., & Marican, S. (2016). The effects of big-five personality traits on deviant behavior. *Procedia - Social and Behavioral Sciences*, *219*(1), 19–25. https://doi.org/10.1016/j.sbspro.2016.04.027

Akour, I. A., Al-Maroof, R. S., Alfaisal, R., & Salloum, S. A. (2022). A conceptual framework for determining metaverse adoption in higher institutions of gulf area: An empirical study using hybrid SEM-ANN approach. *Computers and Education: Artificial Intelligence*, *3*(1), 100052. https://doi.org/10.1016/j.caeai.2022.100052

Al-Abrrow, H., Fayez, A. S., Abdullah, H., Khaw, K. W., Alnoor, A., & Rexhepi, G. (2023). Effect of open-mindedness and humble behavior on innovation: Mediator role of learning. *International Journal of Emerging Markets*, *18*(9), 3065–3084. https://doi.org/10.1108/IJOEM-08-2020-0888

Albayati, H., Alistarbadi, N., & Rho, J. J. (2023). Assessing engagement decisions in NFT Metaverse based on the Theory of Planned Behavior (TPB). *Telematics and Informatics Reports*, *10*(6), 100045. https://doi.org/10.1016/j.teler.2023.100045

Ali, F., El-Manstrly, D., & Abbasi, G. A. (2023). Would you forgive me? From perceived justice and complaint handling to customer forgiveness and brand credibility-symmetrical and asymmetrical perspectives. *Journal of Business Research*, *166*(11), 114138. https://doi.org/10.1016/j.jbusres.2023.114138

Ali, J., Naser Hussain, K., Alnoor, A., Muhsen, Y. R., & Atiyah, A. G. (2024). Benchmarking methodology of banks based on financial sustainability using CRITIC and RAFSI techniques. *Decision Making: Applications in Management and Engineering*, *7*(1), 315–341. https://doi.org/10.31181/dmame712024945

Almarzouqi, A., Aburayya, A., & Salloum, S. A. (2022). Prediction of user's intention to use metaverse system in medical education: A hybrid SEM-ML learning approach. *IEEE Access*. *10*(1), 43421–43434. https://doi.org/10.1109/ACCESS.2022.3169285

Alnoor, A., Tiberius, V., Atiyah, A. G., Khaw, K. W., Yin, T. S., Chew, X., & Abbas, S. (2022). How positive and negative electronic word of mouth (eWOM) affects customers' intention to use social commerce? A dual-stage multi group-SEM and ANN analysis. *International Journal of Human–Computer Interaction*, *40*(3), 808–837. https://doi.org/10.1080/10447318.2022.2125610

Al-Sharafi, M. A., Al-Emran, M., Al-Qaysi, N., Iranmanesh, M., & Ibrahim, N. (2023). Drivers and barriers affecting metaverse adoption: A systematic review, theoretical framework, and avenues for future research. *International Journal of Human–Computer Interaction*. https://doi.org/10.1080/10447318.2023.2260984

Alspach, K. (2022). Why the fate of the metaverse could hang on its security https://venturebeat.com/2022/01/26/why-the-fate-of-the-metaverse-could-hang-on-itssecurity/14March.

Alvarez-Risco, A., Del-Aguila-Arcentales, S., Rosen, M. A., & Yáñez, J. A. (2022). Social cognitive theory to assess the intention to participate in the Facebook Metaverse by citizens in Peru during the COVID-19 pandemic. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(3), 142–156. https://doi.org/10.3390/joitmc8030142

Ameen, N., Hosany, S., & Paul, J. (2022). The personalisation-privacy paradox: Consumer interaction with smart technologies and shopping mall loyalty. *Computers in Human Behavior*, *126*(1), 106976. https://doi.org/10.1016/j.chb.2021.106976

Arpaci, I., & Bahari, M. (2023). Investigating the role of psychological needs in predicting the educational sustainability of Metaverse using a deep learning-based hybrid SEM-ANN technique. *Interactive Learning Environments*. https://doi.org/10.1080/10494820.2022.2164313

Arpaci, I., Karatas, K., Kusci, I., & Al-Emran, M. (2022). Understanding the social sustainability of the Metaverse by integrating UTAUT2 and big five personality traits: A hybrid SEM-ANN approach. *Technology in Society*, *71*(11), 102120. https://doi.org/10.1016/j.techsoc.2022.102120

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, *52*(6), 102063. https://doi.org/10.1016/j.ijinfomgt.2019.102063

Barrera, K. G., & Shah, D. (2023). Marketing in the Metaverse: Conceptual understanding, framework, and research agenda. *Journal of Business Research*, *155*(1), 113420. https://doi.org/10.1016/j.jbusres.2022.113420

Batool, S., & Kashif, M. (2023). Occupational segregation, microaggression, social exclusion, and turnover intentions: Mediating and moderating impact of social invisibility and felt obligation. *International Journal of Sociology and Social Policy*, *43*(7/8), 677–694. https://doi.org/10.1108/IJSSP-07-2022-0190

Belk, R., Humayun, M., & Brouard, M. (2022). Money, possessions, and ownership in the Metaverse: NFTs, cryptocurrencies, Web3 and Wild Markets. *Journal of Business Research*, *153*(1), 198–205. https://doi.org/10.1016/j.jbusres.2022.08.031

Bella, G., Curzon, P., & Lenzini, G. (2015). Service security and privacy as a socio-technical problem. *Journal of Computer Security*, *23*(5), 563–585. https://doi.org/10.3233/JCS-150536

Bostrom, R. P., & Heinen, J. S. (1977a). MIS problems and failures: A socio-technical perspective. Part I: The causes. *MIS Quarterly*, *1*(3), 17–32. https://doi.org/10.2307/248710

Bostrom, R. P., & Heinen, J. S. (1977b). MIS problems and failures: A socio-technical perspective, part II: The application of socio-technical theory. *MIS Quarterly*, *1*(4), 11–28. https://doi.org/10.2307/249019

Buhalis, D., Lin, M. S., & Leung, D. (2022). Metaverse as a driver for customer experience and value co-creation: Implications for hospitality and tourism management and marketing. *International Journal of Contemporary Hospitality Management*, *35*(2), 701–716. https://doi.org/10.1108/IJCHM-05-2022-0631

Burton, S., Lichtenstein, D., Netemeyer, R., & Garretson, J. (1998). A scale for measuring attitude toward private label products and an examination of its psychological and behavioral correlates. *Journal of the Academy of Marketing Science*, *26*(4), 293–306. https://doi.org/10.1177/0092070398264003

Chang, H. H., Wong, K. H., & Lee, H. C. (2022). Peer privacy protection motivation and action on social networking sites: Privacy self-efficacy and information security as moderators. *Electronic Commerce Research and Applications*, *54*(8), 101176. https://doi.org/10.1016/j.elerap.2022.101176

Cheng, X., Mou, J., Shen, X., de Vreede, T., & Raianer, A. (2022). *Call for paper: Opportunities and challenges in the Metaverse*. Internet Research.

Cheung, C. M., Wong, R. Y. M., & Chan, T. K. H. (2021). Online disinhibition: Conceptualization, measurement, and implications for online deviant behavior. *Industrial Management & Data Systems*, *121*(1), 48–64. https://doi.org/10.1108/IMDS-08-2020-0509

Chew, X., Khaw, K. W., Alnoor, A., Ferasso, M., Al Halbusi, H., & Muhsen, Y. R. (2023). Circular economy of medical waste: Novel intelligent medical waste management framework based on extension linear Diophantine fuzzy FDOSM and neural network approach. *Environmental Science and Pollution Research International*, *30*(21), 60473–60499. https://doi.org/10.1007/s11356-023-26677-z

Chu, A. M., & Chau, P. Y. (2014). Development and validation of instruments of information security deviant behavior. *Decision Support Systems*, *66*(1), 93–101. https://doi.org/10.1016/j.dss.2014.06.008

Damar, M. (2021). Metaverse shape of your life for future: A bibliometric snapshot. *Journal of Metaverse*, *1*(1), 1–8. https://doi.org/10.48550/arXiv.2112.12068

Dang, T. T., Dang, K. T., & Küng, J. (2020). Interaction and visualization design for user privacy interface on online social networks. *SN Computer Science*, *1*(5), 1–12. https://doi.org/10.1007/s42979-020-00314-9

De Salve, A., Guidi, B., Ricci, L., & Mori, P. (2018). Discovering homophily in online social networks. *Mobile Networks and Applications*, *23*(6), 1715–1726. https://doi.org/10.1007/s11036-018-1067-2

Dincelli, E., & Yayla, A. (2022). Immersive virtual reality in the age of the Metaverse: A hybrid-narrative review based on the technology affordance perspective. *The Journal of Strategic Information Systems*, *31*(2), 101717. https://doi.org/10.1016/j.jsis.2022.101717

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. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., … Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*(10), 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Dwivedi, Y. K., Kshetri, N., Hughes, L., Rana, N. P., Baabdullah, A. M., Kar, A. K., Koohang, A., Ribeiro-Navarrete, S., Belei, N., Balakrishnan, J., Basu, S., Behl, A., Davies, G. H., Dutot, V., Dwivedi, R., Evans, L., Felix, R., Foster-Fletcher, R., Giannakis, M., … Yan, M. (2023). Exploring the darkverse: A multi-perspective analysis of the negative societal impacts of the metaverse. *Information Systems Frontiers: a Journal of Research and Innovation*, *25*(5), 1–44. https://doi.org/10.1007/s10796-023-10400-x

Ertug, G., Brennecke, J., Kovács, B., & Zou, T. (2022). What does homophily do? A review of the consequences of homophily. *Academy of Management Annals*, *16*(1), 38–69. https://doi.org/10.5465/annals.2020.0230

Falchuk, B., Loeb, S., & Neff, R. (2018). The social metaverse: Battle for privacy. *IEEE Technology and Society Magazine*, *37*(2), 52–61. https://doi.org/10.1109/MTS.2018.2826060

Ferreyra, N. E. D., Hecking, T., Aïmeur, E., Heisel, M., & Hoppe, H. U. (2022). Community detection for access-control decisions: Analysing the role of homophily and information diffusion in Online Social Networks. *Online Social Networks and Media*, *29*(5), 100203. https://doi.org/10.1016/j.osnem.2022.100203

Flavián, C., Ibáñez-Sánchez, S., Orús, C., & Barta, S. (2023). The dark side of the metaverse: The role of gamification in event virtualization. *International Journal of Information Management*, *75*(11), 102726. https://doi.org/10.1016/j.ijinfomgt.2023.102726

Fute, A., Sun, B., & Oubibi, M. (2022). Assessing teaching compassion, work engagement and compassion fatigue among teachers during the pandemic. *Psychology Research and Behavior Management*, *15*(1), 2561–2571. https://doi.org/10.2147/PRBM.S383292

Gao, H., Chong, A. Y. L., & Bao, H. (2023). Metaverse: Literature review, synthesis and future research agenda. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2023.2233455

Go, H., & Kang, M. (2023). Metaverse tourism for sustainable tourism development: Tourism agenda 2030. *Tourism Review*, *78*(2), 381–394. https://doi.org/10.1108/TR-02-2022-0102

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed, a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152. https://doi.org/10.2753/MTP1069-6679190202

Hassouneh, D., & Brengman, M. (2014). A motivation-based typology of social virtual world users. *Computers in Human Behavior*, *33*(4), 330–338. https://doi.org/10.1016/j.chb.2013.08.012

Hichang, C. (2010). Determinants of behavioral responses to online privacy: The effects of concern, risk beliefs, self-efficacy, and communication sources on self-protection strategies. *Journal of Information Privacy and Security*, *6*(1), 3–27. https://doi.org/10.1080/15536548.2010.10855879

Hoang, L. N., & Jung, J. J. (2015). Privacy-aware framework for matching online social identities in multiple social networking services. *Cybernetics and Systems*, *46*(1-2), 69–83. https://doi.org/10.1080/01969722.2015.1007737

Hollenbaugh, E. E., & Everett, M. K. (2013). The effects of anonymity on self-disclosure in blogs: An application of the online disinhibition effect. *Journal of Computer-Mediated Communication*, *18*(3), 283–302. https://doi.org/10.1111/jcc4.12008

Jafar, R. M. S., & Ahmad, W. (2023). Tourist loyalty in the metaverse: The role of immersive tourism experience and cognitive perceptions. *Tourism Review*, *79*(2), 321–336. https://doi.org/10.1108/TR-11-2022-0552

Jung, Y., & Pawlowski, S. D. (2014). Virtual goods, real goals: Exploring means-end goal structures of consumers in social virtual worlds. *Information & Management*, *51*(5), 520–531. https://doi.org/10.1016/j.im.2014.03.002

Kabiri, S., Choi, J., Shadmanfaat, S. M., & Lee, J. (2021). Using structural equations to test a multi-theoretical framework with data on cyberstalking victimization in Iran: Self-control, control deficit, peers' online deviant behaviors, and online deviant lifestyles. *Crime & Delinquency*, *67*(11), 1706–1727. https://doi.org/10.1177/0011128720968501

Kapoor, K., Bigdeli, A. Z., Dwivedi, Y. K., Schroeder, A., Beltagui, A., & Baines, T. (2021). A socio-technical view of platform ecosystems: Systematic review and research agenda. *Journal of Business Research*, *128*(5), 94–108. https://doi.org/10.1016/j.jbusres.2021.01.060

Kar, A. K., & Varsha, P. S. (2023). Unravelling the techno-functional building blocks of Metaverse ecosystems–A review and research agenda. *International Journal of Information Management Data Insights*, *3*(2), 100176. https://doi.org/10.1016/j.jjimei.2023.100176

Kareem, B. A., Zubaidi, S. L., Al-Ansari, N., & Muhsen, Y. R. (2024). Review of recent trends in the hybridisation of preprocessing-based and parameter optimisation-based hybrid models to forecast univariate streamflow. *Computer Modeling in Engineering & Sciences*, *138*(1), 1–41. https://doi.org/10.32604/cmes.2023.027954

Khaw, K. W., Alnoor, A., Al-Abrrow, H., Chew, X., Sadaa, A. M., Abbas, S., & Khattak, Z. Z. (2022). Modelling and evaluating trust in mobile commerce: A hybrid three stage Fuzzy Delphi, structural equation modeling, and neural network approach. *International Journal of Human–Computer Interaction*, *38*(16), 1529–1545. https://doi.org/10.1080/10447318.2021.2004700

Khaw, K. W., Sadaa, A. M., Alnoor, A., Zaidan, A. S., Ganesan, Y., & Chew, X. (2023). Spurring sustainability commitment strategy of family-owned SMEs: A multi-analytical SEM & ANFIS perspective. *The Journal of High Technology Management Research*, *34*(1), 100453. https://doi.org/10.1016/j.hitech.2023.100453

Khedhaouria, A., & Cucchi, A. (2019). Technostress creators, personality traits, and job burnout: A fuzzy-set configurational analysis. *Journal of Business Research*, *101*(8), 349–361. https://doi.org/10.1016/j.jbusres.2019.04.029

Kostick-Quenet, K., & Rahimzadeh, V. (2023). Ethical hazards of health data governance in the metaverse. *Nature Machine Intelligence*, *5*(5), 480–482. https://doi.org/10.1038/s42256-023-00658-w

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, *2*(1), 39–63. https://doi.org/10.1007/s12394-009-0019-1

Lapidot-Lefler, N., & Barak, A. (2012). Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition. *Computers in Human Behavior*, *28*(2), 434–443. https://doi.org/10.1016/j.chb.2011.10.014

Lee, M. K., Cheung, C. M., Lim, K. H., & Ling Sia, C. (2006). Understanding customer knowledge sharing in web-based discussion boards: An exploratory study. *Internet Research*, *16*(3), 289–303. https://doi.org/10.1108/10662240610673709

Lee, C. T., Ho, T. Y., & Xie, H. H. (2023). Building brand engagement in metaverse commerce: The role of branded non-fungible toekns (BNFTs). *Electronic Commerce Research and Applications*, *58*(3), 101248. https://doi.org/10.1016/j.elerap.2023.101248

Lee, J., Kim, J., & Choi, J. Y. (2019). The adoption of virtual reality devices: The technology acceptance model integrating enjoyment, social interaction, and strength of the social ties. *Telematics and Informatics*, *39*(1), 37–48. https://doi.org/10.1016/j.tele.2018.12.006

Li, Y.-J., Cheung, C. M. K., Shen, X.-L., & Lee, M. K. O. (2022). Promoting collaborative learning in virtual worlds: The power of "we". *Information Technology & People*, *36*(6), 2563–2586. https://doi.org/10.1108/ITP-11-2021-0870

Lin, T. C., Huang, S. L., & Hsu, C. J. (2015). A dual-factor model of loyalty to IT product–The case of smartphones. *International Journal of Information Management*, *35*(2), 215–228. https://doi.org/10.1016/j.ijinfomgt.2015.01.001

Lyu, Z. (2023). State-of-the-art human-computer-interaction in Metaverse. *International Journal of Human–Computer Interaction*. https://doi.org/10.1080/10447318.2023.2248833

Muhsen, Y. R., Husin, N. A., Zolkepli, M. B., Manshor, N., & Al-Hchaimi, A. A. J. (2023). Evaluation of the routing algorithms for NoC-based MPSoC: A fuzzy multi-criteria decision-making approach. *IEEE Access*. *11*(1), 102806–102827. https://doi.org/10.1109/ACCESS.2023.3310246

O'Brolcháin, F., Jacquemard, T., Monaghan, D., O'Connor, N., Novitzky, P., & Gordijn, B. (2016). The convergence of virtual reality and social networks: Threats to privacy and autonomy. *Science* *and Engineering Ethics*, *22*(1), 1–29. https://doi.org/10.1007/s11948-014-9621-1

Oh, H. J., Kim, J., Chang, J. J., Park, N., & Lee, S. (2023). Social benefits of living in the metaverse: The relationships among social presence, supportive interaction, social self-efficacy, and feelings of loneliness. *Computers in Human Behavior*, *139*(2), 107498. https://doi.org/10.1016/j.chb.2022.107498

Onofrei, G., Filieri, R., & Kennedy, L. (2022). Social media interactions, purchase intention, and behavioural engagement: The mediating role of source and content factors. *Journal of Business Research*, *142*(3), 100–112. https://doi.org/10.1016/j.jbusres.2021.12.031

Pappas, I. O., & Woodside, A. G. (2021). Fuzzy-set Qualitative Comparative Analysis (fsQCA): Guidelines for research practice in Information Systems and marketing. *International Journal of Information Management*, *58*(6), 102310. https://doi.org/10.1016/j.ijinfomgt.2021.102310

Pedram, S., Ogie, R., Palmisano, S., Farrelly, M., & Perez, P. (2021). Cost–benefit analysis of virtual reality-based training for emergency rescue workers: A socio-technical systems approach. *Virtual Reality*, *25*(4), 1071–1086. https://doi.org/10.1007/s10055-021-00514-5

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *The Journal of Applied Psychology*, *88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Pooyandeh, M., Han, K. J., & Sohn, I. (2022). Cybersecurity in the AI-based metaverse: A survey. *Applied Sciences*, *12*(24), 12993. https://doi.org/10.3390/app122412993

Preece, C., Whittaker, L., & Janes, S. (2022). Choose your own future: The sociotechnical imaginaries of virtual reality. *Journal of Marketing Management*, *38*(15–16), 1777–1795. https://doi.org/10.1080/0267257X.2022.2112610

Rasoolimanesh, S. M., Ringle, C. M., Sarstedt, M., & Olya, H. (2021). The combined use of symmetric and asymmetric approaches: Partial least squares-structural equation modeling and fuzzy-set qualitative comparative analysis. *International Journal of Contemporary Hospitality Management*, *33*(5), 1571–1592. https://doi.org/10.1108/IJCHM-10-2020-1164

Richter, S., & Richter, A. (2023). What is novel about the Metaverse? *International Journal of Information Management*, *73*(12), 102684. https://doi.org/10.1016/j.ijinfomgt.2023.102684

Sadaa, A. M., Ganesan, Y., Khaw, K. W., Alnoor, A., Abbas, S., Chew, X., & Bayram, G. E. (2022). Based on the perception of ethics in social commerce platforms: Adopting SEM and MCDM approaches for benchmarking customers in rural communities. *Current Psychology*, *42*(35), 31151–31185. https://doi.org/10.1007/s12144-022-04069-9

Sarker, S., Chatterjee, S., Xiao, X., & Elbanna, A. (2019). The sociotechnical axis of cohesion for the IS discipline: Its historical legacy and its continued relevance. *MIS Quarterly*, *43*(3), 695–719. https://doi.org/10.25300/MISQ/2019/13747

Sartori, L., & Theodorou, A. (2022). A sociotechnical perspective for the future of AI: Narratives, inequalities, and human control. *Ethics and Information Technology*, *24*(1), 1–11. https://doi.org/10.1007/s10676-022-09624-3

Schütte, R., Ahlemann, F., Becker, J., Legner, C., Lehrer, C., Wiesche, M., & Richter, G. (2022). Quo vadis information systems research in times of digitalization? *Business & Information Systems Engineering*, *64*(4), 529–540. https://doi.org/10.1007/s12599-022-00759-7

Sebastian, G. (2022). A study on Metaverse awareness, cyber risks, and steps for increased adoption. *International Journal of Security and Privacy in Pervasive Computing*, *14*(1), 1–11. https://doi.org/10.4018/IJSPPC.308785

Sebastian, G. (2023). Do ChatGPT and other AI chatbots pose a cybersecurity risk?: An exploratory study. *International Journal of Security and Privacy in Pervasive Computing*, *15*(1), 1–11. https://doi.org/10.4018/IJSPPC.320225

Sengupta, A., & Cao, L. (2022). Augmented reality's perceived immersion effect on the customer shopping process: Decision-making quality and privacy concerns. *International Journal of Retail & Distribution Management*, *50*(8/9), 1039–1061. https://doi.org/10.1108/IJRDM-10-2021-0522

Sharma, T. G., Hamari, J., Kesharwani, A., & Tak, P. (2022). Understanding continuance intention to play online games: Roles of self-expressiveness, self-congruity, self-efficacy, and perceived risk. *Behaviour & Information Technology*, *41*(2), 348–364. https://doi.org/10.1080/0144929X.2020.1811770

Shih, H. P., & Huang, E. (2014). Influences of Web interactivity and social identity and bonds on the quality of online discussion in a virtual community. *Information Systems Frontiers*, *16*(4), 627–641. https://doi.org/10.1007/s10796-012-9376-7

Singla, A., Gupta, N., Aeron, P., Jain, A., Garg, R., Sharma, D., & Arya, V. (2022). Building the Metaverse: Design considerations, socio-technical elements, and future research directions of Metaverse. *Journal of Global Information Management*, *31*(2), 1–24. https://doi.org/10.4018/JGIM.315283

Spector, P. E., Zapf, D., Chen, P. Y., & Frese, M. (2000). Why negative affectivity should not be controlled in job stress research: Don't throw out the baby with the bath water. *Journal of Organizational Behavior*, *21*(1), 79–95. https://doi.org/10.1002/(SICI)1099-1379(200002)21:1<79::AID-JOB964>3.0.CO;2-G

Statista. (2023). "Global digital population as of July 2020". Retrieved August 2, 2023, from https://www.statista.com/statistics/617136/digital-population-worldwide/.

Suh, A., & Cheung, C. M. K. (2019). Revisiting user engagement: Concepts, themes, and opportunities. *PACIS 2019 Proceedings*, 1–15. https://aisel.aisnet.org/pacis2019/150

Tang, J., Akram, U., & Shi, W. (2021). Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: Based on personality traits. *Journal of Enterprise Information Management*, *34*(4), 1097–1120. https://doi.org/10.1108/JEIM-03-2020-0088

Teng, Z., Cai, Y., Gao, Y., Zhang, X., & Li, X. (2022). Factors affecting learners' adoption of an educational metaverse platform: An empirical study based on an extended UTAUT model. *Mobile Information Systems*, *2022*(1), 1–15. https://doi.org/10.1155/2022/5479215

Tseng, H.-T. (2023). Shaping path of trust: The role of information credibility, social support, information sharing and perceived privacy risk in social commerce. *Information Technology & People*, *36*(2), 683–700. https://doi.org/10.1108/ITP-07-2021-0564

Tugtekin, U. (2023). The dark side of metaverse learning environments: Potential threats and risk factors. In *Shaping the future of online learning: Education in the Metaverse* (pp. 57–67). IGI Global.

Valluripally, S., Frailey, B., Kruse, B., Palipatana, B., Oruche, R., Gulhane, A., Hoque, K. A., & Calyam, P. (2023). Detection of security and privacy attacks disrupting user immersive experience in virtual reality learning environments. *IEEE Transactions on Services Computing*, *16*(4), 2559–2574. https://doi.org/10.1109/TSC.2022.3216539

Wan, J., Lu, Y., Wang, B., & Zhao, L. (2017). How attachment influences users' willingness to donate to content creators in social media: A socio-technical systems perspective. *Information & Management*, *54*(7), 837–850. https://doi.org/10.1016/j.im.2016.12.007

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2023). A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials*, *25*(1), 319–352. https://doi.org/10.1109/COMST.2022.3202047

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

Wolter, J. S., & Cronin, Jr, J. J. (2017). Unique influences of cognitive and affective customer-company identification. *Journal of Business Research*, *78*(9), 172–179. https://doi.org/10.1016/j.jbusres.2017.05.010

Wong, R. Y. M., Cheung, C. M. K., & Xiao, B. (2018). Does gender matter in cyberbullying perpetration? An empirical investigation. *Computers in Human Behavior*, *79*(2), 247–257. https://doi.org/10.1016/j.chb.2017.10.022

Wong, L.-W., Tan, G. W.-H., Ooi, K.-B., & Dwivedi, Y. K. (2023). Metaverse in hospitality and tourism: A critical reflection. *International Journal of Contemporary Hospitality Management*. https://doi.org/10.1108/IJCHM-05-2023-0586

Wright, M. F., Harper, B. D., & Wachs, S. (2019). The associations between cyberbullying and callous-unemotional traits among adolescents: The moderating effect of online disinhibition. *Personality and Individual Differences*, *140*(4), 41–45. https://doi.org/10.1016/j.paid.2018.04.001

Yeap, J. A., Ramayah, T., & Soto-Acosta, P. (2016). Factors propelling the adoption of m-learning among students in higher education. *Electronic Markets*, *26*(4), 323–338. https://doi.org/10.1007/s12525-015-0214-x

Zaidan, A. A., Alnoor, A., Albahri, O. S., Mohammed, R. T., Alamoodi, A. H., Albahri, A. S., Zaidan, B. B., Garfan, S., Hameed, H., Al-Samarraay, M. S., Jasim, A. N., & Malik, R. Q. (2023). Review of artificial neural networks-contribution methods integrated with structural equation modeling and multi-criteria decision analysis for selection customization. *Engineering Applications of Artificial Intelligence*, *124*(9), 106643. https://doi.org/10.1016/j.engappai.2023.106643

Zhang, M., Liu, Y., Wang, Y., & Zhao, L. (2022). How to retain customers: Understanding the role of trust in live streaming commerce with a socio-technical perspective. *Computers in Human Behavior*, *127*(2), 107052. https://doi.org/10.1016/j.chb.2021.107052

Zhang, C., Lu, T., Chen, S., & Zhang, C. (2017). Integrating ego, homophily, and structural factors to measure user influence in online community. *IEEE Transactions on Professional Communication*, *60*(3), 292–305. https://doi.org/10.1109/TPC.2017.2703038

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K.-K R. (2022). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *Artificial Intelligence Review*, *55*(2), 1029–1053. https://doi.org/10.1007/s10462-021-09976-0

Zhang, Y., Zhang, M., Luo, N., Wang, Y., & Niu, T. (2019). Understanding the formation mechanism of high-quality knowledge in social question and answer communities: A knowledge co-creation perspective. *International Journal of Information Management*, *48*(10), 72–84. https://doi.org/10.1016/j.ijinfomgt.2019.01.022

Zhang, H., & Zhao, H. (2022). How is virtuous personality trait related to online deviant behavior among adolescent college students in the internet environment? A moderated moderated-mediation analysis. *International Journal of Environmental Research and Public Health*, *19*(15), 1–15. https://doi.org/10.3390/ijerph19159528

Zhou, C., Li, K., & Zhang, X. (2022). Why do I take deviant disclosure behavior on internet platforms? An explanation based on the neutralization theory. *Information Processing & Management*, *59*(1), 102785. https://doi.org/10.1016/j.ipm.2021.102785

About the authors

Chew XinYing is a Senior Lecturer in the School of Computer Sciences, Universiti Sains Malaysia. She holds a Ph.D. in statistical quality control from Universiti Sains Malaysia. Her areas of research are in Industrial Computing, Statistical Quality Control, Advanced Analytics (Machine Learning & Deep Learning).

Victor Tiberius is an honorary professor at the chair of Business and Economics at the University of Potsdam, Germany. His work has been published in journals such as the Journal of Business Research.

Alhamzah Alnoor is a Senior Lecturer at the Southern Technical University, Management Technical College. He received his MBA from the University of Basrah. His research interests lie in organizational studies. He received his PhD from the School of Management, Universiti Sains Malaysia, Penang, Malaysia.

Mark Camilleri is an Associate Professor in the Department of Corporate Communication at the University of Malta. Prof. Camilleri was featured among the world's top 2% of scientists. Prof. Camilleri has been recognized as a "top peer reviewer" by Web of Science.

Khaw Khai Wah is a Senior Lecturer in the School of Management, Universiti Sains Malaysia. He holds a Ph.D. in statistical quality control from Universiti Sains Malaysia. His areas of research are in advanced analytics and statistical quality/process control.