Metaverse Security and Privacy Research: A Systematic Review

Argianto Rahartomo[a], Leonel Merino[b], Mohammad Ghafari[a]

[a]*Technische Universität Clausthal, Goslar, Germany*
[b]*School of Design, School of Engineering, Pontificia Universidad Católica de Chile, Santiago, Chile*

Abstract

The rapid growth of metaverse technologies, including virtual worlds, augmented reality, and lifelogging, has accelerated their adoption across diverse domains. This rise exposes users to significant new security and privacy challenges due to sociotechnical complexity, pervasive connectivity, and extensive user data collection in immersive environments. We present a systematic review of the literature published between 2013 and 2024, offering a comprehensive analysis of how the research community has addressed metaverse-related security and privacy issues over the past decade. We organize the studies by method, examined the security and privacy properties, immersive components, and evaluation strategies. Our investigation reveals a sharp increase in research activity in the last five years, a strong focus on practical and user-centered approaches, and a predominant use of benchmarking, human experimentation, and qualitative methods. Authentication and unobservability are the most frequently studied properties. However, critical gaps remain in areas such as policy compliance, accessibility, interoperability, and back-end infrastructure security. We emphasize the intertwined technical complexity and human factors of the metaverse and call for integrated, interdisciplinary approaches to securing inclusive and trustworthy immersive environments.

Keywords: Metaverse, Privacy, Security

1. Introduction

The metaverse offers unprecedented opportunities to reshape how we engage with digital and physical spaces, powered by advancements in augmented reality, virtual reality, and artificial intelligence. However, as this ecosystem evolves, so do the risks associated with security and privacy vulnerabilities (Huang et al., 2023; Rahartomo et al., 2025). Addressing these challenges is imperative, especially as the metaverse begins to permeate critical domains such as education, healthcare, and commerce.

We conducted a systematic study of 114 metaverse security and privacy papers published between 2013 and 2024, aiming to investigate research methods in this domain. We explored the types of studies conducted, the properties emphasized, the research strategies adopted, and the scope of their evaluations. To ensure the credibility of our findings, we also analyzed common threats to validity across the reviewed studies, identifying recurring risks that may affect the reliability, generalizability, or interpretation of results in metaverse security and privacy research.

We found that the number of publications continues to grow, with a noticeable shift toward technique-driven and evaluation-focused studies. Authentication and confidentiality (*i.e.*, 22 and 12 of 68 articles), are the most widely explored security properties , underscoring their critical role in safeguarding the metaverse. Privacy aspects such as unobservability (hiding a user's actions) and content awareness (ensuring appropriate access to virtual environments) also garnered significant attention (*i.e.*, 14 and 12 of 46 articles) , highlighting a growing concern for user privacy in immersive settings. A substantial proportion of studies (71%) employed multiple research strategies to address the unique complexities of immersive environments, such as evaluating real-world usability, capturing subjective user experiences, and measuring system performance. The most commonly used strategies were benchmarking (30%), human experimentation (26%), and interviews (14%). In total, 69% of the metaverse studies involved human participants, with a median sample size of 25 participants. These studies typically evaluated user performance through metrics such as task completion times

Email addresses: argianto.rahartomo@tu-clausthal.de (Argianto Rahartomo), leonel.merino@uc.cl (Leonel Merino), mohammad.ghafari@tu-clausthal.de (Mohammad Ghafari)

and task accuracy. Our analysis of threats to validity across the reviewed studies uncovered several recurring concerns: limited generalizability stemming from small or unrepresentative samples, insufficient methodological transparency that undermines the reliability of findings, and disalignment between theoretical constructs and their practical implementation.

Our investigation also highlighted several critical gaps in metaverse security and privacy research areas that warrant further investigation.

Infrastructure and Network Protocols: While much of the existing research focuses on virtual and augmented reality (AR / VR) hardware, security and privacy concerns related to back-end infrastructures and network communication protocols have been significantly underexplored, posing potential vulnerabilities in large-scale metaverse systems. Infrastructure and network protocols are essential to the functioning of metaverse systems, but have not received much attention in current research. Some challenges, such as inadequate encryption for real-time communication and inconsistent identity management, pose risks to user privacy and system security. Although emerging solutions, such as more secure communication standards and the implementation of artificial intelligence that preserves privacy, show promise, these approaches are still in the early stages and need further investigation.

Interoperability: Only three studies addressed interoperability between different metaverse platforms. This leaves a critical research gap around how data is exchanged and managed securely across diverse virtual environments, with potential implications for user privacy. In fact, interoperability in the metaverse is based not just on asset portability but also on deep integration at the back-end infrastructure and network protocol level. Current metaverse platforms, such as Horizon Worlds, Decentraland, and Roblox, rely on incompatible server architectures and data models, making real-time cross-platform interaction difficult. Without a standard protocol stack or federated identity system, even basic cross-platform movement could compromise user privacy or system integrity.

Accessibility for Disabilities: The accessibility of the metaverse for users with disabilities or disorders is an overlooked topic. Despite the promise of immersive technologies to enable new forms of interaction, participation, and presence, only one study (Zhao et al., 2019) explicitly addressed the needs of individuals with low vision. This limited attention is particularly concerning given the potential of the metaverse to bridge or widen digital divides, and the unique security risks this user group faces. In addition, immersive devices often lack accessibility features by default, and existing privacy controls may not be adaptable to different perceptual or interaction needs.

Regulatory and Compliance Concerns: Many existing studies overlook critical aspects of metaverse governance, including regulatory frameworks and compliance measures that are essential for protecting user privacy. This oversight risks creating significant gaps in the legal and ethical protections available to users. The metaverse presents substantial social and ethical challenges, especially with respect to data privacy, identity, and digital autonomy. Immersive and persistent virtual environments collect extensive personal and behavioral data, prompting serious concerns about surveillance, informed consent, and data control. The flexible nature of digital identity, where avatars can differ significantly from real-world user personas, further complicates issues of accountability, authenticity, and representation. In the absence of well-defined regulations and ethical standards, these concerns may erode user trust and hinder the widespread adoption of metaverse technologies.

Scalability and Performance Under Load: As the metaverse scales in both user base and technological complexity, ensuring consistent performance becomes a critical challenge. High concurrency, real-time interactions, and the integration of diverse media, such as rich 3D environments and data streams, place immense pressure on the network infrastructure, rendering systems vulnerable to latency, lag, and instability. Additionally, managing distributed computation and maintaining synchronization across heterogeneous devices further complicates scalability.

In summary, our study offers a comprehensive analysis of current trends in metaverse security and privacy research, identifies significant gaps, and highlights critical issues that warrant further investigation. Our findings set the stage for future research, informing efforts to strengthen the security and privacy foundations of this digital ecosystem.

We call on researchers in the field to prioritize accessibility by exploring inclusive design principles, evaluating assistive technologies in extended reality (XR) settings, and developing security and privacy models that accommodate diverse abilities, ensuring equitable and trustworthy participation in metaverse environments. We also urge the community to address regulatory and compliance challenges by examining how different user groups experience risks and by guiding the development of strong privacy protections, identity management systems, and inclusive governance frameworks. Finally, we encourage research on scalability and performance, particularly through adaptive load balancing and decentral-

ized architectures, such as blockchain or peer-to-peer systems, which offer promising solutions to meet the growing demands of metaverse platforms.

The remainder of this article is organized as follows. We describe our research methodology in Section 2. We present and discuss our findings in Section 3. We explain threats to the validity of this study in Section 4 and conclude the article in Section 5.

2. Methodology

We followed the systematic review of the literature (SLR) method, which is highly popular in Software Engineering (Kitchenham et al., 2007). The diagram shown in Figure 1 represents the process we followed for data selection (*i.e.*, identify data sources and establish inclusion and exclusion criteria). Next, we discuss the data extraction process.

2.1. Data selection

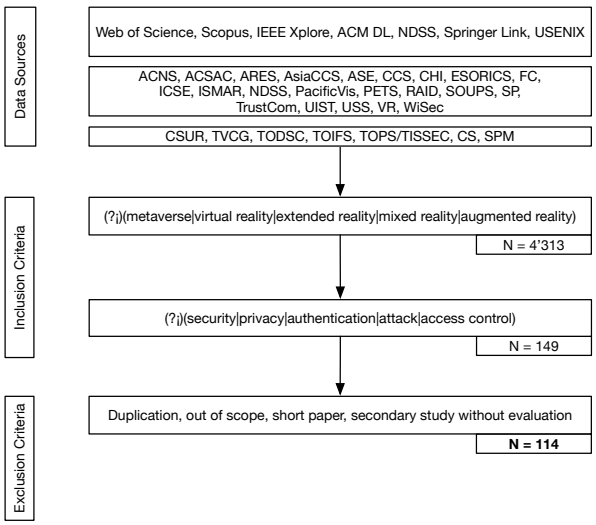

Figure 1: The process for selecting 114 papers that evaluate immersive technologies in security and privacy.

We seek articles that describe evaluations involving immersive technologies (*e.g.*, metaverse, virtual reality, augmented reality) within the domain of security and privacy. To ensure the high quality of primary studies, we examined the best publications, including conference and journal proceedings, on security and privacy, software engineering, and human-computer interaction.

Data sources. We curated a list of venues A *, A and B based on the Core Ranking for conferences[1] and journals[2].

Inclusion criteria. We used popular digital libraries and search engines (*i.e.*, Web of Science[3], Scopus[4], IEEE Xplore[5], ACM DL[6], Springer Link[7]) to identify articles suitable for the scope of the study. Articles published in USENIX and NDSS were not included in these databases, but are made accessible on their respective websites. We selected articles published between 2013 and 2024. We first included papers that contain (in titles, abstracts, or keywords) a metaverse-related keyword, and then included papers that also contain a keyword related to the security and privacy domain. We focused our selection on the top-ranked venues in the security and privacy fields, including USS, SP, CCS, NDSS, CRYPTO, and JoC. From this analysis, after excluding common stop words and nonspecific terms such as *user*, *data*, *system*, and *device*, we identified the five most recurring words relevant to security: *security*, *privacy*, *authentication*, *attack*, and *access control*. We used them to narrow down the results and focus on papers more relevant to the security and privacy domain. We developed a Python script[8] to automate metadata extraction. We used the Computer Science Bibliography (DBLP)[9] to obtain the title of articles when direct access to metadata was not available. Next, we used the titles to retrieve the metadata of the articles using Google Scholar[10]. Then, we manually verified the results to ensure the completeness of the metadata.

Exclusion criteria. Next, we excluded duplicate results (*i.e.*, articles returned by more than one source), short articles for which we included an extended version, and secondary studies without evaluations. We also excluded a study that served primarily as a call for submissions of papers to a conference and some studies that present a systematic taxonomy and classification of specific topics without discussing any form of evaluation method. Finally, we selected 114 papers.

2.2. Data Extraction

For each article, we categorize the details of the metaverse considered, the type of study, the security and pri-

[1] http://portal.core.edu.au/conf-ranks/
[2] http://portal.core.edu.au/jnl-ranks/
[3] https://mjl.clarivate.com/home
[4] https://www.scopus.com/search/form.uri
[5] https://ieeexplore.ieee.org/xplore/home.jsp
[6] https://dl.acm.org/
[7] https://link.springer.com/
[8] https://doi.org/10.5281/zenodo.15738685
[9] https://dblp.org/db/
[10] https://scholar.google.com/

vacy properties, the research strategy used, the characteristics of the evaluations carried out, and threats to validity. The first two authors of the article participated in the extraction process. We calibrated our assessments with a small subset of papers. We discussed the results and solved conflicting classifications. Finally, we independently analyzed the 114 included articles, compared the results, and agreed on the classifications by consensus.

2.2.1. Metaverse Focus

To define the focus of the metaverse, we categorize the components outlined in research and the various forms of reality.

Component. Since there is not 'one' metaverse, we used a popular taxonomy (Smart et al., 2007) to classify the metaverse components described in studies. We classified the components into one of the following four categories. Notice that the *augmented reality* component is not restricted to a specific type of reality, as we will discuss next.

- Virtual Worlds are digital environments in which users interact with each other and with the surroundings through avatars. An example is a study of Lin about preserving avatar's authenticity (Lin et al., 2023).
- Lifelogging involves the ongoing process of recording one's own data of experiences and daily activities, often using wearable devices. One example is a study by DeVrio about utilizing the smartwatch for real-time tracking of user's gesture and activity (DeVrio et al., 2023).
- Augmented Reality refers to the process of superimposing digital information or objects on the real world. An example is a study by Lehman about the privacy risks of augmented reality (Lehman et al., 2022).
- Mirror World is about creating digital replicas of the real world, accurately reproducing real-life locations, events, and objects. An example is a study by Maddali and Lazar on how to understand the social context to create meaningful reconstructions of physical spaces for remote instruction and interaction (Maddali and Lazar, 2023).

Reality Type. We adopted the definitions of the types of reality described in the mixed reality continuum (Milgram and Kishino, 1994). We extended the definitions to include extended reality (Esen et al., 2023) We classified each article on the basis of explicit descriptions of various types of reality. Those articles mentioning the term *metaverse* without specifying a particular type of reality were classified as *XR* (Torres et al., 2023).

- Virtual reality (VR) is an artificial digital environment that provides an immersive experience to users, often simulating real-world interactions through multisensory feedback. Examples of VR include interactive 3D games like Minecraft VR and professional applications such as virtual training simulators for education and healthcare.
- Augmented Reality (AR) is a technology that enhances the real world by overlaying digital information such as sound, video, graphics, or GPS data on it, and an example of AR is the Timetraveler app, which allows users to experience historical events through augmented visuals and sounds at specific locations.
- Mixed Reality (MR) is an interactive technology that blends real-world and virtual elements, where digital and physical objects coexist and interact in real-time, and an example of MR is the Microsoft HoloLens which offers a hybrid of real and virtual experiences by projecting holograms into the user's environment.
- Extended Reality (XR) is a collective term for immersive technologies such as Virtual Reality (VR), Augmented Reality (AR) and Mixed Reality (MR) that enhance or replace the physical world with digital elements, exemplified by headsets that overlay holograms on the real world or fully immersive simulations.

2.2.2. Study Type

We classified the 114 research articles based on Munzner's framework (Munzner, 2008), which we adjusted to the scope of our study, into one of five types:

Applications. Studies that describe the use of existing metaverse techniques in order to solve a concrete and relevant problem in the security and privacy domain. That is, these papers do not present novel techniques but focus on design decisions during the development process. Artifacts are often available to promote the reproducibility of the results. When found, we classified these artifacts into the following categories:

- Application Code (AC) refers to the source code and accompanying documentation necessary for

the installation and execution of a software program;

- Experimental Data (ED) refers to supplemental materials, including datasets and other artifacts that are utilized in experiments; and
- Executable Applications (EX) are compiled programs that can be run but cannot be altered.

Evaluations. Studies that concentrate on the assessment of applications, often involving users. Evaluations can involve various methodologies, such as case studies, user studies, and controlled experiments. Depending on the goal of an evaluation, they can collect and analyze data such as user performance or user experience.

Models. Papers that, for example, introduce formalisms to describe new abstractions, definitions, or terminology to characterize methods or analyze phenomena. Models also include taxonomies for classifications to understand a particular subject and can involve commentaries in which the authors of a paper present arguments to support a position.

Systems. Studies that focus on the architecture of a framework or toolkit designed to support the development of applications. Unlike applications, systems do not address a particular security and privacy property but rather a type of problem.

Techniques. Papers that provide comprehensive explanations of the supporting algorithms and technical descriptions of the implementations. Often, techniques are aimed at efficiency and performance (*e.g.*, to reduce memory usage, reduce processing time, or improve overall performance) and are evaluated using benchmarks to compare with state-of-the-art techniques.

2.2.3. Security and Privacy Property

To classify the articles, we used the security and privacy properties that arise when building software, proposed in a previous popular study (De Guzman et al., 2019b). We determined the most prominent category by analyzing the descriptions of the threat or privacy model, which we often found explicitly in a dedicated section of articles.

Authentication. It checks the legitimacy of users who access the metaverse device or service, allowing only authenticated users to progress to the identification and authorization steps. An exemplary study by George investigates the use of 3D spatial user behavior as an authentication method for smart homes in virtual and real realities (George et al., 2019).

Confidentiality. Protects sensitive data from unauthorized access by implementing rigorous access controls to personal and identifiable information. A notable study highlights the assumed confidentiality in VR interactions and advocates for enhanced security protocols (Gopal et al., 2023).

Authorization and access control. It requires that actions and processes be initiated only by verified parties with appropriate access levels, guaranteeing that only authorized apps can interact with specified data or objects. Current authorization models for mixed reality platforms expose vulnerabilities in 3D spatial maps, which shows the need for stronger access control mechanisms (Farrukh et al., 2023).

Integrity. It relates to ensuring that data and processes in metaverse environment remain unchanged and accurate, allowing for the proper detection and display of virtual augmentations without unauthorized changes. For example, the integrity of avatars can be enhanced through visual indicators to identify abusive ad service providers in virtual environments (Lin et al., 2023).

Identification. It entails assigning each action within metaverse system to a specific entity, hence easing access management and avoiding unwanted actions by ensuring all participants are recognized. For example, the characteristics of the user's gait can be used for their identification, which requires a balance between recognition accuracy and preservation of privacy in virtual environments (Hanisch et al., 2023).

Availability. It emphasizes the importance of ongoing access to data and services within a metaverse application, to prevent attackers from impeding these resources. An exemplary study of Rovira proposed a high availability system architecture to guarantee consistent content access (Rovira et al., 2013).

Non-repudiation. It ensures that if an action is taken or data are modified within metaverse application, the entity responsible cannot deny their involvement, hence establishing accountability via digital evidence. For example, data provenance can be used to trace and display cyberattack patterns, providing detailed forensic trails from initial reconnaissance to system exploitation, thus ensuring non-repudiation (Garae et al., 2017).

Unobservability & Undetectability. Protects entities' presence or activity from detection by attackers, ensuring that activities remain secret and indistinguishable from noise. For example, personal data can be concealed by playing in an 'escape room' scenario, demonstrating the effectiveness of unobservability and undetectability in protecting privacy (Nair et al., 2023b).

Content Awareness. It ensures that users are completely aware of the nature and sensitivity of the data they share, fostering transparency and informed consent. In fact, there is a need to integrate user perspectives and privacy considerations in XR design, in particular, how content awareness can enhance user engagement and data protection (Maddali and Lazar, 2023).

Anonymity & Pseudonymity. It enables entities to separate or disguise their identities from data or actions, providing privacy while preventing adversaries from tracing activities back to individuals. For example, the GaitLock system integrates innovative gait recognition techniques based on dynamic time warping and sparse representation classifier to advance pseudonymity (Shen et al., 2019).

Policy & Consent Compliance. Ensures a system to comply with specified privacy and security rules, ensuring that user rights are respected and enforced. For example, there are significant privacy topics Oculus with VR applications, which requires a thorough reassessment of policy frameworks to better protect user data (Trimananda et al., 2022).

Unlinkability. Prevents adversaries from linking an entity to specific data or behaviors, protecting privacy by hiding linkages between user activities. An exemplary study by Patan and Parizi, combines encryption with blockchain technology to protect against data breaches and obscures personal data from unauthorized inference (Patan and M. Parizi, 2023).

Plausible Deniability. It allows entities to plausibly deny involvement in actions or data storage while providing privacy protection against data origin tracing. For example, spatial augmented reality (SAR) (Huang and Ling, 2022), proposes a new methodological strategy to achieve plausible deniability by offering robust privacy protections in digital environments.

2.2.4. Research Strategy

We identify the research strategies adopted in studies based on the empirical software engineering standards of the ACM (ACM, 2021; Hasselbring, 2021; Ralph, 2021).

Benchmarking. Comparison of the efficacy of various methods, tools, or techniques in real-world contexts. Typically, it compares the study with previous works. For example, benchmarks can be used to evaluate the reliability of an authentication model over time (Luo et al., 2020).

Human Experimentation. Engages users in testing or model development and observes the effects of deliberate interventions under controlled conditions to study aspects of reality. For example, an experiment can help to assess the experiences of adolescents and potential security threats from various perspectives (Deldari et al., 2023).

Qualitative Survey (Interviews). Consists of semi-structured or open-ended interviews for data collection. It is explicitly mentioned in the papers. For example, interviews could be used to investigate user reactions to perceptual manipulation attacks (Cheng et al., 2023).

Questionnaire Surveys. Collects responses to a structured series of questions using digital or on-line questionnaires. It is also explicitly mentioned in the papers. For example, questionnaires can be used to explore the usability and security of authentication mechanisms in a virtual reality (VR) setting (Mathis et al., 2021).

Data Science. Apply data-centered methodologies, including machine learning algorithms and models for data analysis and interpretation, to examine software engineering phenomena. For example, data science methodologies such as machine learning and deep learning have been instrumental in analyzing motion data from more than 50,000 users (Nair et al., 2023a).

Engineering Research. Focuses on the creation and evaluation of technological artifacts, including algorithms, systems, tools, and other computer-based technologies. For example, this approach was used to examine the APIs of wallets in different applications and websites to identify possible data breaches (Torres et al., 2023).

Meta Science. Analyzes research methodologies or offers guidelines for the execution of research, including taxonomy studies. For example, a taxonomy was created to categorize authentication techniques for AR headsets (Düzgün et al., 2022).

2.2.5. Evaluation Scope

We review the scope of evaluations in metaverse security and privacy by collecting data from scenarios in which evaluations are conducted, extracting their quality focus, characteristics of the subjects involved, and the use of research artifacts.

Scenario. To characterize evaluations, we classify the scenarios involved into four types.

- Algorithm Performance entails employing quantitative methods, frequently through benchmarks, to assess the effectiveness and occasionally the efficiency of algorithms, focusing on aspects such as speed and resource usage. For example, they compare results with other approaches and evaluate constraints and behaviors across different data volumes and complexities. Often, such evaluations analyze the algorithm's relative speed, scalability, and performance in extreme circumstances.
- User Experience focuses on capturing the internal state of users when interacting with a technology. This type of scenarios collect data ranging from initial impressions to long-term usage assessments. Such evaluations usually involve the use of surveys and interviews, which often collect data using metrics such as the Likert scale. The data collected can involve aspects such as usability, intuitiveness, trust, and overall satisfaction of the tool, as well as the identification of potential gaps in the tool's functionality and design. Such evaluations might range from informal feedback meetings to systematic usability testing and thorough field observations, providing immediate and in-depth insights on user experiences.
- Understanding Environments and Work Practices relate to assessments to obtain requirements with the goal of understanding the security and privacy needs of users and organizations before developing a metaverse-related approach. Common data collection methods used to understand environments and work practices are observations, surveys, and interviews.
- User Performance assesses measurable factors such as completion time and error rates, alongside quantifiable qualitative assessments. These evaluations may involve user studies that transform real-world tasks into constrained activities, with the aim of either widespread participation to generalize the findings or concentrating on smaller cohorts to deeply understand a specific phenomenon.

Quality Focus. It refers to the key aspects of primary concern in an experiment. These include the specific variables that will be measured, such as the accuracy of the results, the usability of the system, the robustness of its adaptability, and the speed with which tasks can be completed. For example, the quality focus of the study by Liebers is on correctness and robustness (Liebers et al., 2021).

Subject. We collect data from the subject being evaluated, which frequently involves study participants. For example, the study by Lin evaluates the authenticity of the avatar in the context of 60 participants (Lin et al., 2023). In addition, in evaluations that do not involve participants, we collected information on software systems and data sets.

Artifact. We collect involved artifacts such as compiled applications and their source code, as well as experimentation data sets. In addition, we collect information about frameworks and programming languages described in the evaluations. Usually, we find these data in the implementation sections or by analyzing project repositories. In repositories, we found information such as programming languages and frameworks. We consider this information helpful for practitioners and researchers in the field to identify actionable tools and assess their maturity level.

2.2.6. Threat to Validity

In addition, we collect data on threats that often affect the validity of the results of security and privacy studies in the metaverse. Such threats represent risks that can result in findings that are not accurate or trustworthy. We differentiate threats to validity (TTV) from limitations, as limitations refer to constraints or shortcomings in the design or execution of the study. Limitations could affect the interpretation or applicability of the results, but do not necessarily invalidate them. We concentrate on threats to validity because they affect the accuracy or credibility of findings, while we exclude limitations because they affect the extent or conditions under which the findings could be useful.

We note that TTVs are occasionally stated explicitly, frequently in a specific section. While in other studies there may be implicit information that allows us to deduce TTVs. We plan to label explicit and implicit data. To ensure validity, we involved five people from our institution who double-checked the classification of 10% of the collected studies. For each study, we classify TTVs into four categories based on popular frameworks (Wohlin et al., 2024; Campbell and Cook, 1979).

Specifically, we used the following categories: i) threats to internal validity, ii) threats to external validity, iii) threats to conclusion validity, and iv) threats to construct validity.

Threats to internal validity. Threats to internal validity are factors that can lead to incorrect conclusions about causal relationships in a study, such as whether changes in the independent variable truly caused the observed changes in the dependent variable. Such threats arise when alternative explanations for the results are possible due to flaws in the study design or execution. Frequent examples involve participants who show improvement because of practice or experience adverse effects (such as fatigue or boredom) during an experiment. Other examples, include unforeseen events or uncommon circumstances arising during the study, or challenges related to the selection of participants and dropout rates.

Threats to external validity. Threats to external validity are factors that limit the generalizability of study findings beyond the specific conditions of the investigation. That is, they pose a risk, as the outcomes might not be valid in various contexts, populations, or time periods. Common examples involve participants who are not representative of the larger population, the setting of the study (*e.g.*, lab, online) may not reflect real-world conditions, or the findings may only be valid at the time the study was conducted.

Threats to conclusion validity. Threats to the validity of conclusions are factors that could affect the precision and reliability of conclusions about the relationship between variables, especially whether a relationship exists at all. That is, these threats influence the correct interpretation of statistical evidence regarding a relationship. Common threats arise in studies that lack sufficient sample size to detect a true effect, statistical tests that assume certain conditions (*e.g.*, normality, independence), which may not be valid, or when treatments are applied differently among participants.

Threats to construct validity. Threats to construct validity are factors that diminish the extent to which a research study precisely measures or manipulates the theoretical ideas (constructs) it claims to examine. That is, even if an effect is observed in a study, these threats challenge whether the effect pertains to the actual concept investigated. Common examples occur when the concept studied is either vaguely or inconsistently defined, measured, or manipulated using a single method, or evaluated with just one measurement technique.

3. Results and Discussion

Table 1 lists the 114 selected articles, and Figure 2 shows their distribution over time. In the stacked bar chart, the articles published in security & privacy (SP) venues are colored orange, software engineering (SE) venues are colored yellow, while those in human-computer interaction venues (HCI) appear in light blue. We observe that most papers have been published in the last five years (*i.e.*, 78.95%). In the past five years, there has been a significant increase in research focused on metaverse security and privacy. This improvement can be driven by metaverse unique risks, such as user authentication challenges (Stephenson et al., 2022) and the potential for user impersonation (Yang et al., 2023). In addition, emerging threats such as harassment (Dwivedi et al., 2023), identity theft, and data misuse (Pooyandeh et al., 2022) have also contributed to increased attention. In HCI venues, the number of papers has increased moderately in the last three years. The growth in HCI research is supported by advances in hardware, including the release of Meta Quest 2 in 2020, as well as a growing engagement in the community of VR/AR software developers.

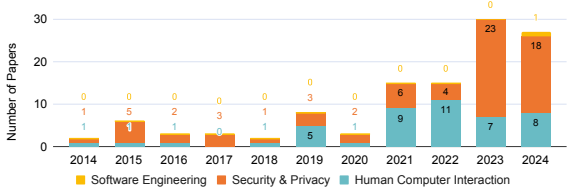

Figure 2: The 114 included papers by publication year and domain.

Table 2 shows a summary of the 114 articles included in the study. We notice that most studies are spread across evaluation (40), technique (39) and application (26) categories, with only a handful focused on models (5) and systems (4). It appears that security and privacy research in the metaverse is more practically oriented, focusing on impact rather than creating new conceptual frameworks, architectures, or theoretical advancements. This practical orientation may signal a shift toward real-world applicability, suggesting a gradual maturation of metaverse security and privacy research. The observed predominance of authentication-focused studies suggests that the metaverse research community is still addressing foundational challenges related to user verification and secure access in immersive environments. This emphasis reflects the early-stage nature of many XR platforms, where reliable identification mechanisms are a prerequisite for trust, personal-

Table 1: List of 114 Included Papers.

Year		Title	Venue
2024	(Cao et al., 2024)	Understanding Parents' Perceptions and Practices Toward Children's Security and Privacy in Virtual Reality	SP
	(Luo et al., 2024)	Eavesdropping on Controller Acoustic Emanation for Keystroke Inference Attack in Virtual Reality	NDSS
	(Slocum et al., 2024)	That Doesn't Go There: Attacks on Shared State in Multi-User Augmented Reality Applications	USS
	(Nguyen et al., 2024)	Penetration Vision through Virtual Reality Headsets: Identifying 360-degree Videos from Head Movements	USS
	(Yang et al., 2024)	Can Virtual Reality Protect Users from Keystroke Inference Attacks?	USS
	(Cheng et al., 2024)	When the User Is Inside the User Interface: An Empirical Study of UI Security Properties in Augmented Reality	USS
	(Zhang et al., 2024a)	Exploring the Design Space of Optical See-through AR Head-Mounted Displays to Support First Responders in the Field	CHI
	(Kyu et al., 2024)	EITPose: Wearable and Practical Electrical Impedance Tomography for Continuous Hand Pose Estimation	CHI
	(Katins et al., 2024)	Assessing User Apprehensions About Mixed Reality Artifacts and Applications: The Mixed Reality Concerns (MRC) Questionnaire	CHI
	(Abraham et al., 2024)	What You Experience is What We Collect: User Experience Based Fine-Grained Permissions for Everyday Augmented Reality	CHI
	(Liebers et al., 2024)	Kinetic Signatures: A Systematic Investigation of Movement-Based User Identification in Virtual Reality	CHI
	(Hadan et al., 2024)	Privacy in Immersive Extended Reality: Exploring User Perceptions, Concerns, and Coping Strategies	CHI
	(Guo et al., 2024)	An Empirical Study on Oculus Virtual Reality Applications: Security and Privacy Perspectives	ICSE
	(Mollyn and Harrison, 2024)	EgoTouch: On-Body Touch Input Using AR/VR Headset Cameras	UIST
	(Rack et al., 2024)	Motion Passwords	VR
	(Kumar et al., 2024)	A Generative Framework for Low-Cost Result Validation of Machine Learning-as-a-Service Inference	AsiaCCS
	(Alghamdi et al., 2024)	¡italic¿xr-droid¡/italic¿: A Benchmark Dataset for AR/VR and Security Applications	TODSC
	(Liu et al., 2024)	Time to Think the Security of WiFi-Based Behavior Recognition Systems	TODSC
	(Li et al., 2024)	Dangers Behind Charging VR Devices: Hidden Side Channel Attacks via Charging Cables	TOIFS
	(Zhang et al., 2024b)	An Anti-Disguise Authentication System Using the First Impression of Avatar in Metaverse	TOIFS
	(Wilson et al., 2024)	Privacy-Preserving Gaze Data Streaming in Immersive Interactive Virtual Reality: Robustness and User Experience	TVCG
	(Nair et al., 2024)	Berkeley Open Extended Reality Recordings 2023 (BOXRR-23): 4.7 Million Motion Capture Recordings from 105,000 XR Users	TVCG
	(Wan et al., 2024)	Analysis and Design of Efficient Authentication Techniques for Password Entry with the Qwerty Keyboard for VR Environments	TVCG
	(Riyadh et al., 2024)	Usable Authentication in Virtual Reality: Exploring the Usability of PINs and Gestures	ACNS
	(Hamici-Aubert et al., 2024)	Leveraging Overshadowing for Time-Delay Attacks in 4G/5G Cellular Networks: An Empirical Assessment	ARES
	(Singha et al., 2024)	Securing Contrastive mmWave-based Human Activity Recognition against Adversarial Label Flipping	WiSec
	(Sabra et al., 2024)	De-anonymizing VR Avatars using Non-VR Motion Side-channels	WiSec
2023	(Farrukh et al., 2023)	LocIn: Inferring Semantic Location from Spatial Maps in Mixed Reality	USS
	(Kim et al., 2023)	Erebus: Access Control for Augmented Reality Systems	USS
	(Slocum et al., 2023)	Going through the motions: AR/VR keylogging from user head motions	USS
	(Rajaram et al., 2023b)	Reframe: An Augmented Reality Storyboarding Tool for Character-Driven Analysis of Security & Privacy Concerns	UIST
	(Lin et al., 2023)	Visual Indicators Representing Avatars' Authenticity in Social Virtual Reality and Their Impacts on Perceived Trustworthiness	TVCG
	(Nair et al., 2023a)	Unique Identification of 50, 000+ Virtual Reality Users from Head & Hand Motion Data	USS
	(Torres et al., 2023)	Is Your Wallet Snitching On You? An Analysis on the Privacy Implications of Web3	USS
	(Zhang et al., 2023b)	It's all in your head(set): Side-channel attacks on AR/VR systems	USS
	(Kaplan et al., 2023)	A Tagging Solution to Discover IoT Devices in Apartments	ACSAC
	(Nair et al., 2023b)	Exploring the Privacy Risks of Adversarial VR Game Design	PETS
	(Gallardo et al., 2023)	Speculative Privacy Concerns About AR Glasses Data Collection	PETS
	(Windl et al., 2023)	Investigating Security Indicators for Hyperlinking Within the Metaverse	SOUPS
	(Deldari et al., 2023)	An Investigation of Teenager Experiences in Social Virtual Reality from Teenagers', Parents', and Bystanders' Perspectives	SOUPS
	(Munsinger et al., 2023)	Virtual reality for improving cyber situational awareness in security operations centers	CS
	(Maddali and Lazar, 2023)	Understanding Context to Capture when Reconstructing Meaningful Spaces for Remote Instruction and Connecting in XR	CHI
	(Cheng et al., 2023)	Exploring User Reactions and Mental Models Towards Perceptual Manipulation Attacks in Mixed Reality	USS
	(Hanisch et al., 2023)	Understanding Person Identification Through Gait	PETS
	(Vondráček et al., 2023)	Rise of the Metaverse's Immersive Virtual Reality Malware and the Man-in-the-Room Attack & Defenses	CS
	(Rajaram et al., 2023a)	Eliciting Security & Privacy-Informed Sharing Techniques for Multi-User Augmented Reality	CHI
	(Patan and M. Parizi, 2023)	Securing Data Exchange in the Convergence of Metaverse and IoT Applications	ARES
	(Wu et al., 2023)	Privacy Leakage via Unrestricted Motion-Position Sensors in the Age of Virtual Reality: A Study of Snooping Typed Input on Virtual Keyboards	SP
	(Wang et al., 2023)	Low-effort VR Headset User Authentication Using Head-reverberated Sounds with Replay Resistance	SP
	(Zhu et al., 2023)	SoundLock: A Novel User Authentication Scheme for VR Devices Using Auditory-Pupillary Response	NDSS
	(Gopal et al., 2023)	Hidden Reality: Caution, Your Hand Gesture Inputs in the Immersive Virtual World are Visible to All!	USS
	(Zhang et al., 2023a)	FaceReader: Unobtrusively Mining Vital Signs and Vital Sign Embedded Sensitive Info via AR/VR Motion Sensors	CCS
	(Nair et al., 2023c)	Going Incognito in the Metaverse: Achieving Theoretically Optimal Privacy-Usability Tradeoffs in VR	UIST
	(DeVrio et al., 2023)	SmartPoser: Arm Pose Estimation with a Smartphone and Smartwatch Using UWB and IMU Data	UIST
	(Yang et al., 2023)	A Secure Authentication Framework to Guarantee the Traceability of Avatars in Metaverse	TOIFS
	(Liu et al., 2023b)	MagLoc-AR: Magnetic-Based Localization for Visual-Free Augmented Reality in Large-Scale Indoor Environments	TVCG
	(Li et al., 2023)	SigA: RPPG-Based Authentication for Virtual Reality Head-Mounted Display	RAID
2022	(Trimananda et al., 2022)	OVRSEEN: Auditing Network Traffic and Privacy Policies in Oculus VR	USS
	(Li et al., 2022)	NailRing: An Intelligent Ring for Recognizing Micro-gestures in Mixed Reality	ISMAR
	(Lehman et al., 2022)	Hidden in Plain Sight: Exploring Privacy Risks of Mobile Augmented Reality Applications	TOPS
	(Sykownik et al., 2022)	Something Personal from the Metaverse: Goals, Topics, and Contextual Factors of Self-Disclosure in Commercial Social VR	CHI
	(Tseng et al., 2022)	The Dark Side of Perceptual Manipulations in Virtual Reality	CHI
	(Stephenson et al., 2022)	SoK: Authentication in Augmented and Virtual Reality	SP
	(Mathis et al., 2022)	Virtual Reality Observations: Using Virtual Reality to Augment Lab-Based Shoulder Surfing Research	VR
	(Mathis et al., 2022)	Can I Borrow Your ATM? Using Virtual Reality for (Simulated) In Situ Authentication Research	VR
	(Düzgün et al., 2022)	SoK: A Systematic Literature Review of Knowledge-Based Authentication on Augmented Reality Head-Mounted Displays	ARES
	(Lehrbaum et al., 2022)	Enabling Customizable Workflows for Industrial AR Applications	ISMAR
	(Miller et al., 2022a)	Combining Real-World Constraints on User Behavior with Deep Neural Networks for Virtual Reality (VR) Biometrics	VR
	(Luo et al., 2022)	HoloLogger: Keystroke Inference on Mixed Reality Head Mounted Displays	VR
	(Huang and Ling, 2022)	SPAA: Stealthy Projector-based Adversarial Attacks on Deep Image Classifiers	VR
	(Miller et al., 2022b)	Temporal Effects in Motion Behavior for Virtual Reality (VR) Biometrics	VR
	(Meteriz-Yildiran et al., 2022)	A Keylogging Inference Attack on Air-Tapping Keyboards in Virtual Environments	VR
2021	(Gordon et al., 2021)	Covert Embodied Choice: Decision-Making and the Limits of Privacy Under Biometric Surveillance	CHI
	(Dudley et al., 2021)	Crowdsourcing Design Guidance for Contextual Adaptation of Text Content in Augmented Reality	CHI
	(Lee et al., 2021)	AdCube: WebVR Ad Fraud and Practical Confinement of Third-Party Ads	USS
	(Pereira et al., 2021)	ARENA: The Augmented Reality Edge Networking Architecture	ISMAR
	(Liebers et al., 2021)	Understanding User Identification in Virtual Reality Through Behavioral Biometrics and the Effect of Body Normalization	CHI
	(Mathis et al., 2021)	RepliCueAuth: Validating the Use of a Lab-Based Virtual Reality Setup for Evaluating Authentication Systems	CHI
	(Vergari et al., 2021)	Influence of Interactivity and Social Environments on User Experience and Social Acceptability in Virtual Reality	VR
	(Casey et al., 2021)	Immersive Virtual Reality Attacks and the Human Joystick	TODSC
	(Li et al., 2021a)	Kal epsilon ido: Real-Time Privacy Control for Eye-Tracking Systems	USS
	(Miller et al., 2021)	Using Siamese Neural Networks to Perform Cross-System Behavioral Authentication in Virtual Reality	VR
	(Arafat et al., 2021)	VR-Spy: A Side-Channel Attack on Virtual Key-Logging in VR Headsets	VR
	(David-John et al., 2021)	A privacy-preserving approach to streaming eye-tracking data	TVCG
	(Vo-Huu et al., 2021)	Spectrum-flexible secure broadcast ranging	WiSec
	(Li et al., 2021b)	Designing Leakage-Resilient Password Entry on Head-Mounted Smart Wearable Glass Devices	TOIFS
	(Lu et al., 2021)	Global Feature Analysis and Comparative Evaluation of Freestyle In-Air-Handwriting Passcode for User Authentication	ACSAC
	(Harborth and Frik, 2021)	Evaluating anpd redefining smartphone permissions with contextualized justifications for mobile augmented reality apps	SOUPS
2020	(Luo et al., 2020)	OcuLock: Exploring Human Visual System for Authentication in Virtual Reality Head-mounted Display	NDSS
	(John et al., 2020)	The Security-Utility Trade-off for Iris Authentication and Eye Animation for Social Virtual Avatars	TVCG
	(Khan et al., 2020)	Mimicry Attacks on Smartphone Keystroke Authentication	TOPS
2019	(Ruth et al., 2019)	Secure Multi-User Content Sharing for Augmented Reality Applications	USS
	(George et al., 2019)	Investigating the Third Dimension for Authentication in Immersive Virtual Reality and in the Real World	VR
	(Bozkir et al., 2019)	Person Independent, Privacy Preserving, and Real Time Assessment of Cognitive Load using Eye Tracking in a Virtual Reality Setup	VR
	(Zhao et al., 2019)	Designing AR Visualizations to Facilitate Stair Navigation for People with Low Vision	UIST
	(Sun et al., 2019)	Collaborative Visual Analysis with Multi-level Information Sharing Using a Wall-Size Display and See-Through HMDs	PACIFICVIS
	(Xu et al., 2021)	Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality	CHI
	(De Guzman et al., 2019a)	A First Look into Privacy Leakage in 3D Mixed Reality Data	ESORICS
	(Shen et al., 2019)	GaitLock: Protect Virtual and Augmented Reality Headsets Using Gait	TODSC
2018	(Lebeck et al., 2018)	Towards Security and Privacy for Multi-user Augmented Reality: Foundations with End Users	SP
	(Pham, 2018)	Human Identification Using Neural Network-Based Classification of Periodic Behaviors in Virtual Reality	VR
	(Adams et al., 2018)	Ethics emerging: The story of privacy and security perceptions in virtual reality	SOUPS
2017	(Lebeck et al., 2017)	Securing Augmented Reality Output	SP
	(Sluganovic et al., 2017)	HoloPair: Securing Shared Augmented Reality Using Microsoft HoloLens	ACSAC
	(Garae et al., 2017)	Visualizing the New Zealand Cyber Security Challenge for Attack Behaviors	TrustCom
2016	(Figueiredo et al., 2016)	Prepose: Privacy, Security, and Reliability for Gesture-Based Programming	SP
	(Hartl et al., 2016)	Efficient verification of holograms using mobile augmented reality	TVCG
	(Xu et al., 2016)	Virtual U: Defeating Face Liveness Detection by Building Virtual Models From Your Public Photos	USS
2015	(Vilk et al., 2015)	SurroundWeb: Mitigating Privacy Concerns in a 3D Web Browser	SP
	(Ens et al., 2015)	Candid Interaction: Revealing Hidden Mobile and Wearable Computing Activities	UIST
	(Yadav et al., 2015)	Design and Analysis of Shoulder Surfing Resistant PIN Based Authentication Mechanisms on Google Glass	FC
	(Lantz et al., 2015)	Visual Cryptography and Obfuscation: A Use-Case for Decrypting and Deobfuscating Information Using Augmented Reality	FC
2014	(Denning et al., 2014)	In situ with bystanders of augmented reality glasses: perspectives on recording and privacy-mediating technologies	CHI
	(Roesner et al., 2014)	World-Driven Access Control for Continuous Sensing	CCS

ization, and safety. In addition, the growing number of practical evaluations, especially user studies and benchmarking, indicates a shift from conceptual exploration to applied research that tests real-world usability, effectiveness, and security results. This trend toward empirical validation may signify the maturation of the field, as

researchers increasingly prioritize deployable solutions over theoretical models. It also underscores the need for methodological rigor and cross-disciplinary collaboration to ensure that emerging systems are not only secure, but also usable, inclusive, and adaptable to diverse contexts of adoption.

Our findings indicate that authentication (22) and unobservability (14) are the most frequently studied security and privacy properties, respectively. They are frequently observed in multiple techniques (11 and 8) and evaluations (7 and 4), but are rarely seen in applications (2 and 1). This suggests that research is currently focusing on broader aspects of authentication and unobservability rather than specific issues, perhaps because these specific issues have yet to be identified. We observe that research efforts are evenly distributed across metaverse components such as virtual worlds (74), lifelogging (56), and augmented reality (55); this is consistent with virtual (66) and augmented (55) reality being the terms most frequently encountered in studies. The relatively even distribution of research across metaverse components, such as virtual worlds, lifelogging, and augmented reality, suggests a broad and exploratory phase in the development of metaverse security and privacy research. Rather than coalescing around a dominant platform or technology, the field is actively investigating risks and design considerations across a variety of immersive paradigms. This diversity may reflect the fragmented nature of current metaverse technologies, where no single platform or interaction model has yet emerged as a clear standard. It also highlights the importance of tailoring security and privacy solutions to the specific advantages and vulnerabilities of each component, for example, continuous sensing in AR, persistent data collection in lifelogging, or identity persistence in virtual worlds. As the metaverse continues to evolve, this balanced research landscape provides a foundation for comparative studies and the eventual development of cross-platform security frameworks that can accommodate heterogeneous environments. All technique articles reported the use of benchmarking research strategies, and some (8) also describe methods that involve the evaluation of user performance and experience, which shows the need for comprehensive evaluations. The exclusive reliance on benchmarking in technique-oriented papers, with only a minority incorporating user performance or experience evaluations, highlights a gap in how technical contributions are validated in metaverse security and privacy research. This suggests a need for more comprehensive evaluation strategies that not only measure technical efficiency but also consider usability, user perception, and real-world applicability, factors that are crucial in immersive and interactive systems. Both evaluation and application papers place a strong emphasis on users. Evaluations integrate a combination of human experimentation (41), interviews (26), and questionnaires (24). This aligns with the numerous applications and techniques focused on optimizing algorithm performance, as well as evaluations focused on user performance and experience. We also identified several studies (50) that evaluated the environment and work practices, reflecting a pragmatic approach focused on grasping the specific requirements when integrating metaverse technologies to meet security and privacy demands.

Table 3 presents a more detailed list of the 26 venues in which included studies are published.[11] We notice that SE publications are only in one venue and HCI publications are largely confined to only six venues, in contrast to SP papers, which are spread across 19 venues. Possibly due to the rapid progression of the metaverse, we observe that most studies (*i.e.*, 82%) are published at conferences (which offer expedited review processes) rather than through journals to facilitate timely dissemination of findings.

- In the last decade, security and privacy risks in metaverse publications increased from 2 to 27 yearly, evidencing greater attention to community research.
- Conference publications are almost five times more than journal publications (*i.e.*, 20 and 94, respectively), which could be attributed to a quick evaluation process in conferences aligning with the rapid advancement of the metaverse.
- The 44% of the studies evaluated the environment and work practices, suggesting a practical approach to address security and privacy issues in the metaverse.

3.1. Metaverse Focus

Figure 3 displays the results related to the components of the metaverse. Each colored line corresponds to a specific metaverse component. The *Y* axis shows the percentage associated with each component, and the circles are marked with the count of studies involving those components. In particular, there is a consistent decline

[11] We investigated a total of 68 conferences and journals each year, from 2013 to 2024.

Table 2: The number of papers by ranked venues.

Type	Virtual World	Lifelogging	Augmented Reality	Mirror World	Metaverse	Virtual Reality	Augmented Reality	Mixed Reality	Extended Reality	Reality	Authentication	Confidentiality	Authorization	Integrity	Identification	Availability	Non-repudiation	Security	Unobservability	Content Awareness	Anonymity	Policy	Unlinkability	Deniability	Privacy	Benchmarking	Human Experimentation	Interview	Questionnaire	Data Science	Engineering Research	Meta Science	Strategy	Algorithm Performance	Environment and Practices	User Experience	User Performance	Evaluation	Total
Application	15	11	15	6	13	15	4	3		2	3	4	3	2	1	2		1	2	1	3	1	1		14	14	2	9	4	4	0		16	11	7	7		**26**
Evaluation	27	13	16	7	24	16	3	3		7	5	3	1	4	0	0		4	10	2	3	1	0		5	27	24	15	4	2	1		6	31	15	13		**40**
Model	3	2	2	3	2	2	1	1		2	0	0	1	1	0	0		1	0	0	0	0	0		4	0	0	1	2	1	2		4	1	0	0		**5**
System	1	2	3	2	0	3	1	1		0	1	2	0	0	0	0		0	0	0	0	1	0		3	0	1	0	0	1	0		2	2	0	0		**4**
Technique	28	28	19	12	27	19	7	2		11	3	1	5	2	2	0		8	0	5	0	1	1		39	16	3	4	16	1	0		39	5	6	8		**39**
Total	74	56	55	30	66	55	16	10		22	12	10	10	9	3	2		14	12	8	6	4	2		65	57	30	29	26	9	3		67	50	28	28		**114**

Table 3: Selected Publication Venues.

No	Name	Included
1	IEEE Transactions on Visualization and Computer Graphics	8
2	IEEE Transactions on Dependable and Secure Computing	4
3	IEEE Transactions on Information Forensics and Security	4
4	ACM Transactions on Privacy and Security	2
5	Computers and Security	2
6	Usenix Security Symposium	17
7	International Conference on Human Factors in Computing Systems	16
8	IEEE Conference on Virtual Reality and 3D User Interfaces	14
9	IEEE Symposium on Security and Privacy	8
10	ACM Symposium on User Interface Software and Technology	6
11	Symposium On Usable Privacy and Security	4
12	IEEE/ACM International Symposium on Mixed and Augmented Reality	3
13	Usenix Network and Distributed System Security Symposium	3
14	Privacy Enhancing Technologies Symposium	3
15	Annual Computer Security Applications Conference	3
16	International Conference on Availability, Reliability and Security	3
17	ACM Conference on Security and Privacy in Wireless and Mobile Networks	3
18	ACM Conference on Computer and Communications Seurity	2
19	Financial Cryptography and Data Security Conference	2
20	IEEE Pacific Visualization Symposium	1
21	European Symposium on Research in Computer Security	1
22	Asia Conference on Information, Computer and Communications Security	1
23	The International Symposium on Research in Attacks, Intrusions and Defenses	1
24	International Conference on Trust, Security and Privacy in Computing and Communications	1
25	International Conference on Applied Cryptography and Network Security	1
26	International Conference on Software Engineering	1
	Total	114

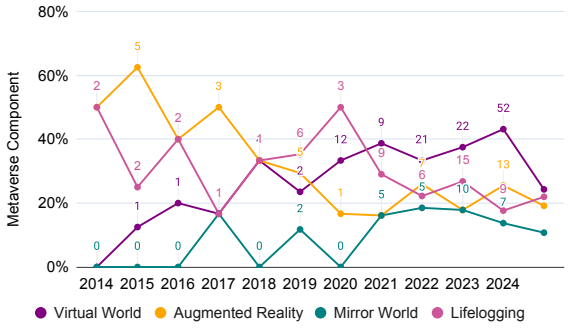

Figure 3: The evolution of metaverse components.

in augmented reality, while virtual worlds show a steady rise. The total number of studies has increased significantly in recent years, and in the last two years, the percentages of different components have converged. In the past, the total number of studies was relatively small, with a higher percentage using AR probably due to smartphones being more accessible than VR headsets. Today, VR headsets have gained popularity and immersive AR headsets are available, although they are quite expensive. We anticipate that future research will focus on integrating various elements, as devices such as the Meta Quest 3 have made AR and VR more economically accessible. Figure 4 illustrates a stacked bar chart that shows the distribution of metaverse components engaged in evaluating various security and privacy properties. Most of these evaluations (*i.e.*, 42%) focus on a single metaverse component. However, some (*i.e.*, 37%) involve two, and a small fraction (*i.e.*, 12%) incorporate three components. Properties like integrity, authentication, and unobservability often engage virtual worlds, whereas authentication, authorization, confidentiality, content awareness are associated with augmented reality.

Mirror worlds appear infrequently in evaluations, whereas lifelogging is more prominent in properties related to unobservability & undetectability, and identification. Possibly, complex social and economic interactions through avatars (Wu et al., 2023; Nair et al., 2023c) in virtual worlds promote the investigation of security properties such as authentication and data integrity. However, the need for advanced mapping technologies and geospatial data (Farrukh et al., 2023) to develop mirror worlds makes it more challenging to incorporate them into security and privacy experiments. These factors could contribute to the fact that mirror worlds are less frequently included in evaluations of se-

curity and privacy properties compared to other metaverse components.

- In the last two years, the number of publications that involve virtual worlds (*i.e.*, 24%), lifelogging (*i.e.*, 22%), augmented reality (*i.e.*, 19%), and mirror worlds (*i.e.*, 11%), has almost converged.
- In 42% of the cases, the evaluations focus on one component of the metaverse.
- Typically, virtual worlds are evaluated for properties such as authentication (*i.e.*, 27%), unobservability (*i.e.*, 15%) and integrity (*i.e.*, 11%). Lifelogging is often evaluated based on authentication (*i.e.*, 20%), unobservability (*i.e.*, 20%) and identification (*i.e.*, 13%). Augmented reality tends to be analyzed in terms of authentication (*i.e.*, 15%), confidentiality (*i.e.*, 15%), and authorization (*i.e.*, 15%). Mirror worlds evaluations usually involve authentication (*i.e.*, 20%), unobservability (*i.e.*, 20%), and anonymity (*i.e.*, 10%).

There is an interesting observation in authorization. We can see that 57% of the studies focused on authorization involve AR, but only 14% involve virtual worlds. This is likely due to differences in the interaction and environmental contexts. In AR, devices and software have a feature known as perceptual sensing. This refers to the ability of hardware or software to continuously monitor the physical environment using cameras and other sensors (Roesner et al., 2014). Due to this capability, AR devices can unintentionally capture sensitive information, such as credit card numbers or the contents of computer screens. In addition, the current design of permission models in the underlying operating systems exacerbates the issue of overprivileged access (Kim et al., 2023).

In the context of lifelogging, studies emphasize properties such as unobservability & undetectability, as well as anonymity & pseudonymity, with approximately 35% and 33% of articles addressing these properties, respectively. This focus is understandable given the frequent use of pseudo-identities linked to user profiles for personalized services. However, properties such as policy compliance and consent management remain underexplored and pose significant challenges. This difficulty arises from two main factors: regulatory and technical perspectives (Wilkowska et al., 2023). From a regulatory point of view, regulations such as the GDPR make it difficult to obtain explicit and unambiguous consent from data subjects before processing their data. From a technical perspective, obtaining fully informed consent is challenging because many devices lack screens, making it difficult to display privacy policies.

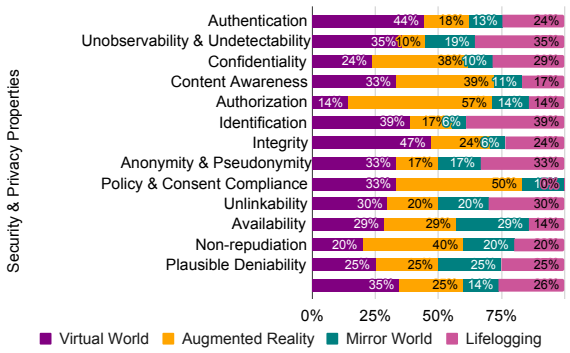

Figure 4: The distribution of metaverse components based on security and privacy properties.

3.2. *Study Type*

Table 2 presents a summary of the classification of papers by type. The colors highlight the dimensions being analyzed. A stronger color intensity indicates a larger number of papers discovered. Evaluation and technique papers are the most common types. These types of paper often employ human experimentation (27) and benchmarking (39) methods. It is important to note that human experimentation does not feature at all in model and system papers, highlighting the difficulties of engaging human participants in testing theories and developing frameworks. Figure 5 presents a line chart with the trends in the percentage of paper types over time. The labels next to the marks indicate the absolute number of papers. The patterns slightly mirror a funnel shape. Specifically, in the early years examined, there were considerable variations in all categories. However, in recent times, there has been a marked decrease in the percentage of applications and techniques, while evaluations have risen moderately and systems have experienced modest growth. In contrast, the absolute number of all types is increasing. Papers on models are almost absent. The emphasis may have shifted due to the urgent need for rapid advances in the metaverse and its inherent complexity (Yu et al., 2023). This situation poses a challenge in creating models that remain pertinent and precise enough for comprehensive testing and validation, as foundational technology evolves quickly. In addition, the presence of software and immersive hard-

ware allows for user assessments and the validation of existing methods' effectiveness.

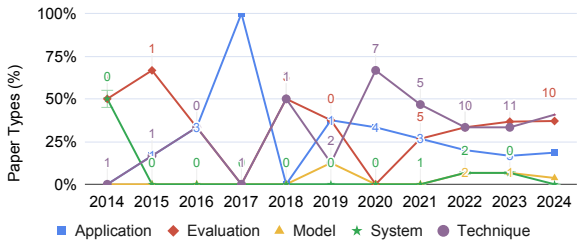

Figure 5: Trends of the types of papers per year.

- Although the total quantity in all types of paper continues to increase, indicating a vibrant landscape, the technique and evaluation paper have received more attention in recent years.
- The nearly lack of models found (*i.e.*, 4%) emphasize the urgent need to develop a common understanding of the foundations to approach security and privacy concerns in the metaverse.

3.3. Security & Privacy Property

Figure 6 presents a stacked bar chart with the total number of paper types by security and privacy properties. We found a small but consistent number of application papers for all security & privacy properties with the exception of unobservability & undetectability and identification. Real-world usage contexts and direct interactions with users may influence properties like unobservability & undetectability, and identification. Evaluating these properties requires empirical data, which can only be obtained through practical scenarios such as user studies, surveys, or case studies. These strategies may provide insight into how these properties function under actual conditions. Therefore, it is not surprising that evaluation papers tend to explore these properties in greater depth. In contrast, application papers often lack the scope to conduct empirical studies or extensive surveys. We observe that multiple techniques address authentication (11) and unobservability & undetectability (8), integrity (5), and anonymity & pseudonymity (5). The prominence of authentication may suggest that security and privacy concerns persist in metaverse development. In effect, the strong focus on authentication across the reviewed studies reflects the nascent and infrastructure-building stage of metaverse technology adoption. As platforms strive to attract broader user bases and support increasingly complex interactions, the ability to reliably identify and verify users becomes fundamental. Unlike traditional web or mobile ecosystems, metaverse environments require continuous and often multimodal authentication through biometrics, behavioral signals, or embodied interactions, which introduces both technical challenges and privacy risks. The emphasis of the research community on authentication likely mirrors industry priorities, where trust, security, and prevention of impersonation are immediate concerns in enabling social, commercial, and enterprise use cases. This also suggests that before metaverse technologies can evolve towards richer, large-scale, and interoperable systems, the field must first establish robust identity frameworks that account for the unique characteristics of immersive, embodied interaction. Authentication techniques are essential to ensure that system or application access is restricted to verified users, thus preventing unauthorized entry. Thus, authentication is a vital attribute in the research on techniques that protect data and transactions in metaverse applications. For example, *SigA* (Li et al., 2023) is an innovative technique that uses a physiological signal that is invisible to the naked eye (photoplethysmogram) rather than the more commonly used electro-oculogram and electrical muscle stimulation methods for authentication. The technique improves security by reducing the risk of shoulder surfing attacks and strengthens user privacy by mitigating the threats posed by side-channel attacks. In addition to security and privacy, it is also worth to consider authentication from other perspectives, including deployability, usability, and accessibility.

We identified several papers (12) that address content awareness; however, none are classified as technique-type papers. Content awareness is often discussed in studies that emphasize user interaction, such as evaluation or application. In contrast, technique papers generally focus on solutions to specific issues, such as security or privacy-enhancing algorithms, without paying much attention to user experience. Consequently, aspects such as transparency and user awareness regarding the data they share are frequently neglected. The absence of content awareness in technique-type papers indicates a disconnect between technical solutions and user-facing concerns such as transparency and informed consent. This suggests that technical research on metaverse security may overlook critical aspects of user experience, potentially limiting the trustworthiness and adoption of proposed solutions. Bridging this gap requires integrating user-centered principles into the de-

sign and evaluation of security and privacy-enhancing technologies.

We found that most evaluations focus on content awareness (10), authentication (7), confidentiality (5), unobservability & undetectability (4), and identification (4). We did not find evaluations that focus on properties such as availability, non-repudiation, and plausible deniability. Limited research on, for example, anonymity and pseudonymity can be attributed to the complexity of privacy issues (Liu et al., 2023a). One contributing factor to this complexity is the low level of user awareness (Tseng et al., 2022). Awareness typically develops over time and is influenced by users' experiences with the technology itself. Without a proper understanding of privacy risks, users often underestimate the importance of privacy protection features in the metaverse. Therefore, two important aspects must be addressed: the development of technology that leverages user privacy and the need to raise user awareness about the risks present in the metaverse.

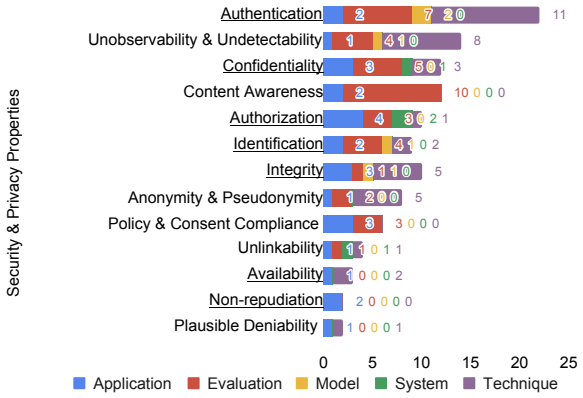

Figure 6: Security & privacy properties involved in metaverse evaluations by paper types. The labels on security properties are underlined.

Figure 7 presents a stacked area chart with the evolution of the number of articles by security and privacy properties. Regardless of specific properties, there has been a steady increase in the number of research papers on metaverse security and privacy. In the past three years, there has been a notable increase in articles dealing with authentication, unobservability and undetectability, confidentiality, and content awareness. Similarly, this field is expanding as the number of relevant topics grows, highlighting a broad focus on various security and privacy properties. In addition, there has been a notable increase in privacy-focused articles in the last three years.

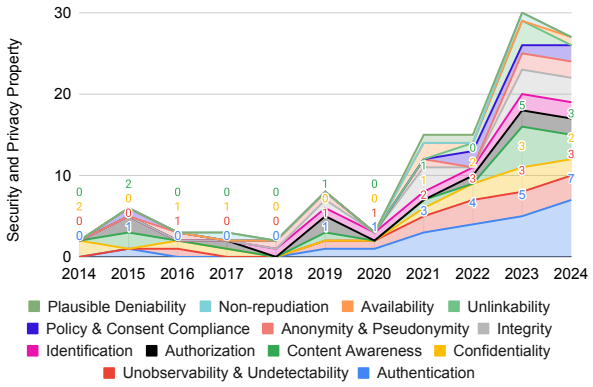

Figure 7: The evolution of security & privacy properties between 2014 and 2024.

- Authentication and confidentiality are the most common security properties (*i.e.*, 22 and 12 of 68 articles), while unobservability and content awareness are the most common privacy properties (*i.e.*, 14 and 12 of 46 articles).
- The field of security and privacy in the metaverse is growing, with research increasingly diversifying into a larger number of security and privacy properties over time.

3.4. Research Strategy

Figure 8 illustrates the evolution of research strategies used to assess aspects of security and privacy within the metaverse. Each colored line presents the evolution of the percentage of studies related to a specific research strategy over a year. The labels on the marks display the total number of studies that employ the research strategy. Notice that we collected all research strategies described in the articles and often found investigations that involve more than one strategy. Approximately 29% employ a single strategy, around 50% incorporate two, and the remaining 21% use three strategies. These findings could correspond to the complexity of immersive environments, where numerous variables can influence user behavior, highlighting the need for various methods in evaluations. There is a significant increase in the number of strategies included in the investigation (in line with the increasing number of studies), with strategies becoming more evenly distributed over the past two years.

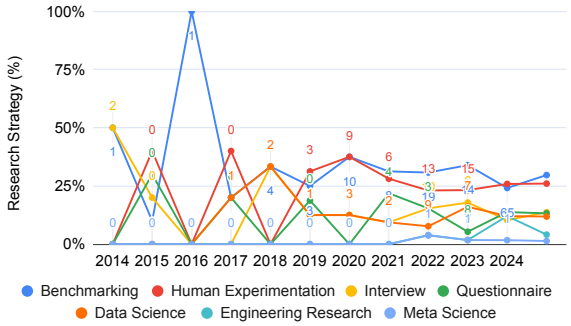

Figure 8: The evolution of research strategies used in the evaluation of security and privacy within the metaverse.

- The top 3 research strategies used to study security and privacy in the metaverse include benchmarking, human experiments, and interviews, accounting for 30%, 26%, and 14% of usage, respectively.
- 71% percent of the studies involve more than one research strategy, highlighting the complexity of immersive environments where numerous variables can influence user behavior, underscoring the need for various evaluation methods.

3.5. Evaluation Scope

Table 4 presents an exhaustive list of the scope of the evaluations in the 114 articles analyzed. We collect various details of the evaluations, such as the scenarios in which they occur (*e.g.*, algorithm performance, environment and work practices, user experience and performance), the scope of the studies and information about available artifacts. We observe that most evaluations (*i.e.*, 67%) include human subjects. The widespread integration of real-world datasets along with accessible application artifacts highlights the progress towards practical reliability. In general, these results suggest that the focus on user-centered methods guarantees the reliability and relevance of these technologies in actual settings.

Figure 9 presents a Sankey diagram with the distribution of the number of studies that involved the main aspects analyzed. In it, each column presents one of the dimensions analyzed (*i.e.*, evaluation scenarios, paper types, publication venues, security & privacy properties, and types of reality). We observe that technique papers typically validate their approaches focusing on

Table 4: Evaluation and Quality Metrics.

Property	Algorithm Performance	User Performance	User Experience	Environment and Practices	Correctness	Usability	Robustness	Time	Average	Std. Dev
	Evaluation				Quality				Participants	
Authentication	13	9	8	8	13	11	8	6	37.0	36.0
Unobservability & Undetect.	12	1	4	3	11	4	9	0	15.1	14.3
Confidentiality	7	3	3	6	5	7	3	4	26.5	33.8
Content Awareness	0	3	5	12	0	12	0	0	59.0	70.1
Authorization	5	1	1	5	2	5	5	0	4.8	8.0
Identification	6	3	2	5	5	3	5	1	112.7	269.4
Integrity	8	3	2	4	7	2	4	5	22.9	27.9
Anonymity & Pseudonymity	6	2	0	1	5	1	3	0	68.1	160.4
Policy & Consent Compliance	2	2	2	4	1	3	2	0	55.0	115.1
Unlinkability	3	0	0	1	2	2	1	2	6.8	5.4
Availability	3	0	0	0	1	0	2	1	266.7	461.9
Non-repudiation	1	0	1	0	1	1	0	0	10.5	14.8
Plausible Deniability	1	1	0	1	1	0	1	1	27.5	38.9
Total	67	28	28	50	55	51	44	20	54.8	133.4

algorithm performance scenarios, whereas articles centered on evaluations mostly focus on user experience. The application papers present a more balanced mix of evaluation scenarios, assessing both the algorithm performance and the performance and experience of the users. We observed that papers in venues for human-computer interaction, such as the CHI conference, predominantly emphasize evaluations. In contrast, those in the TVCG journal and the IEEE VR conference are more technique-oriented. Articles published in security & privacy venues, often target the USS and SP conferences, which display a balanced distribution of applications, evaluations, and techniques. Our analysis reveals that authentication is the property most frequently examined in security-related papers. These studies frequently incorporate virtual reality. Although a significant number of these papers appear in IEEE VR, many are distributed across various other venues.

Scenario. Figure 10 illustrates the evolution of the evaluation scenarios over the years. Since 2018, there has been a significant increase in the evaluation of user experience, user performance, and algorithm performance scenarios. It is quite interesting because, in previous years, growth in these scenarios was not as high as in the past six years. This shift can be attributed to the increased efforts of the community and advances in technology. According to Stone and Chapman, the accessibility of technological developments, such as eye track-

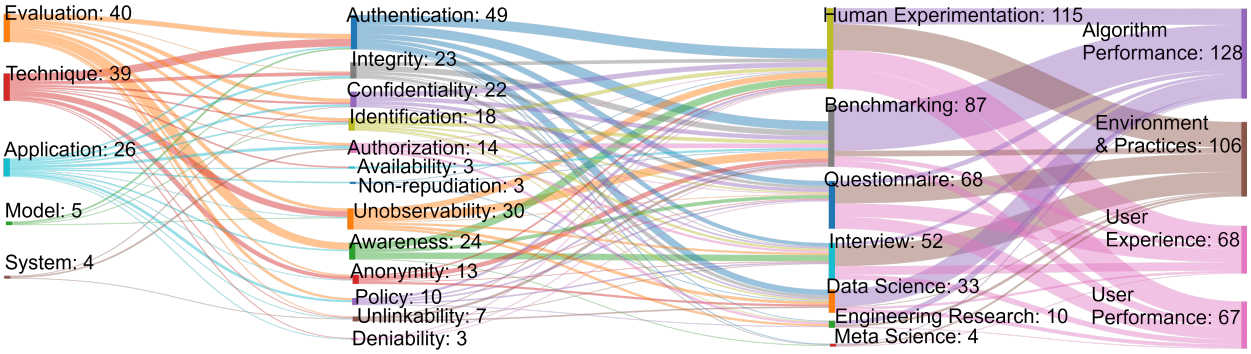

Figure 9: Relationship between evaluation scenarios, study types, venues, S&P properties, type of reality.

ing devices, mouse tracking devices, and similar tools, has contributed to this increase (Stone and Chapman, 2023). Moreover, the availability of software development kits (SDKs) and libraries, such as Microsoft's Mixed Reality Toolkit and open-source solutions from Pupil Labs since 2017–2018, has also played an important role in driving this growth.

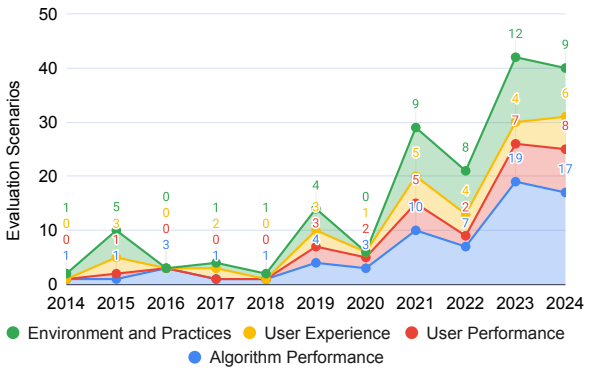

Figure 10: The evolution of the number of evaluation scenarios over the years.

Quality Focus. We note that correctness and usability are the main emphasis in metaverse evaluations. Specifically, of the 55 studies that highlight usability, a limited number also address correctness (10), robustness (10), and time (5). Similarly, in the 55 studies that focus on correctness, several also consider robustness (21) and time (12). We think these results highlight the complexity of evaluating usability together with user performance. We notice that usability directly connects to user engagement and improves user compliance with privacy (Andrabi et al., 2015; Nair et al., 2023c) However, evaluating usability typically requires creating an intuitive interface that helps users understand system processes, ensures their continuous engagement, and encourages compliance with privacy guidelines, presenting a significant challenge for these evaluations. We note that half of studies (11) that relate to authentication concentrate on usability. The remaining studies examine both correctness and robustness and time. For example, a study by George evaluates a method of selecting objects in three dimensions to enhance usability and security in authentication, in order to prevent shoulder surfing attacks (George et al., 2019). Authentication in metaverse application is different from web-based system. The inclusion of additional devices, such as headsets, makes evaluating the usability of authentication methods important. Last but not least, there are three authentication studies focused on the three aspects of quality. A study by Yadav focuses on designing shoulder surf-resistant PIN-based authentication mechanisms for Google Glass, using both voice-based and touch-based methods (Yadav et al., 2015). A study by Wilson analyzes privacy mechanisms for gaze data in VR, achieving re-identification accuracy as low as 14% while maintaining high usability and task performance (Wilson et al., 2024). In addition, a study by Lu provides a detailed analysis of authentication using global features from in-air handwriting signals (Lu et al., 2021). In addition, there has been limited focus on topics like policy, which address attacks such as identity theft (Lebeck et al., 2017; Vondráček et al., 2023). We notice that studies that emphasize correctness and robustness instead of completion time focus on reliability and effectiveness over speed in evaluating security and privacy. Often, such studies are related to unobservability, which mitigates risks in identification models, typically aiming to minimize leakage and misuse risks while enhancing defenses against inference attacks.

- 69% of the studies analyzed involve human subjects, often focusing on aspects of user performance, such as the time needed by participants to complete security and privacy tasks and the level of accuracy they achieved.

Subject. We collect data from user studies focusing on the metaverse and security. Often, these participants were involved in creating models to evaluate specific performance metrics, such as authentication or attacks. Figure 11 presents the ratio of female participants to the total number of participants in the studies. Of the 80 user studies, only 57 provided gender data. In addition, we use two colors to visually differentiate the data, each representing security and privacy paper. We note that most studies (*i.e.*, 47 studies) have fewer than 50 participants and at least half are women. We found a median of 25 participants, of which 11 were female (median value). We observe that the sample sizes in metaverse security and privacy studies seem larger than MR/AR (median of 19 with 4 females) (Merino et al., 2020), and in HCI (median of 12) (Caine, 2016) in general. No significant differences were observed in the distribution between the security and privacy user studies, as shown in the graph.

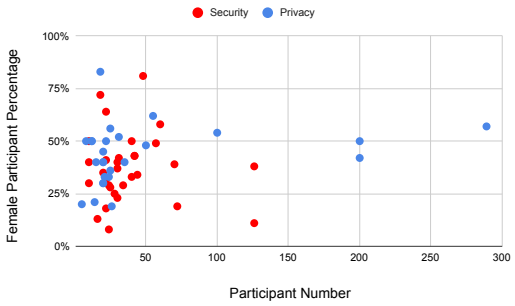

Figure 11: The sample sizes of female participants of 57 of the 80 user studies.

In summary, we observed that techniques typically involve algorithm performance evaluations (*i.e.*, 39 studies), while studies centered on evaluations focus mainly on environmental practices (*i.e.*, 31 studies), user experience (*i.e.*, 15 studies), and user performance (*i.e.*, 13 studies). Applications present a more balanced mix of evaluation scenarios, assessing both algorithm performance (*i.e.*, 16 studies) and user performance and experience (*i.e.*, 14 studies). This trend highlights the diverse focus of research on metaverse technologies, emphasizing the importance of tackling both technical and user-centric challenges.

- 25 of the 114 studies implemented an open source tool such as Unity, which they made public, for instance, through an MIT license.
- The sample sizes in metaverse security and privacy studies (median 25) appear larger than in MR / AR (median 19) and HCI (median 12).

Artifact. Table 5 presents details on the artifacts contained in the repositories. We added links in the URL column to repositories that contain source code, executable applications, or data sets. We confirmed that Python is the most frequent programming language, followed by C#, JavaScript, and Java. We observe that only a few repositories have multiple stars and forks, which shows their limited relevance. The column *license* specifies the type of license and describes how the software can be used, modified, and distributed. Most repositories specifically have an open source license, MIT being the most frequent one. We note that OVRSeen has two licenses. Whereas most files are licensed under MIT, there are a few under GPLv3. It means that whereas most of the files of the systems allow for proprietary use and redistribution with minimal requirements (MIT), a few require that any derivative work be open-source and distributed under the same GPLv3 terms. LGPLv3 is a less restrictive copyleft license allowing linking with non-GPL software, and BSD-3-Clause is permissive like MIT but includes an additional non-endorsement clause. There are six projects without a type of license, its omission means that authors retain all rights of their source code and no one may reproduce, distribute, or create derivative works from their work, which can discourage use and contribution. The column *archive* shows whether a GitHub repository has been archived by its owner, indicating that it is no longer under active maintenance. Once archived, the repository's issues, pull requests, code, and other features become read-only. Contributors can only fork or star the project and cannot make direct changes unless it is unarchived.[12]. Interestingly, two repositories have been explicitly archived, while we notice that many others have been inactive for a long time. The column *running* indicates the duration between the first commit and the most recent update. A prominent example is the *HMD Eyes* project, which is very popular

[12] https://docs.github.com/en/repositories/archiving-a-github-repository/archiving-repositories

with 154 stars and 64 forks. This project showcases an open source eye-tracking platform called Pupil[13] built with the Unity3D engine, specifically for Head-Mounted Displays (HMD). Pupil is developed by Pupil Labs[14], a company focused on investigating hardware and software for eye-tracking. Pupil offers libraries, including an API, under the Pupil Core service, which is developed using the Python programming language. By integrating this platform with Unity3D, the developer aims to enhance the utility of the library, particularly in the metaverse application. We notice that certain projects have a notably brief duration (under two months). `TagApp` and `MetaDataStudy` are extreme examples, all of their contributions occurring in a single day. In addition, some studies have been found to involve multiple repositories. Only the repository with the most stars will be highlighted, indicating its importance. We confirmed that Unity is the most frequently utilized immersive framework, probably because of its active community.

3.6. Potential Issues Affecting Validity

The results of the classification of the threats to validity (TTV) of the 114 studies are presented in Figure 12. In the chart, we encode threats to internal validity in blue, threats to external validity in red, and threats to construct validity in orange. We found that threats to internal validity are the most frequent category (*i.e.*, 50%), and did not find any studies that describe threats to conclusion validity.

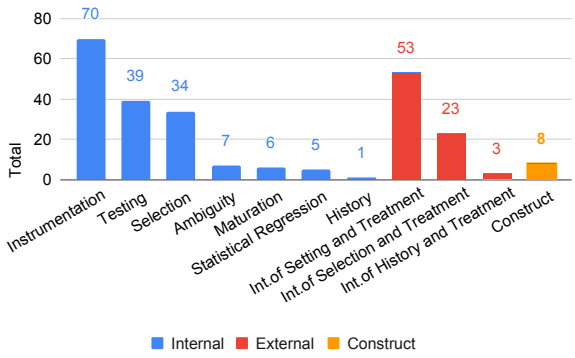

Figure 12: Classification of TTV.

Internal Validity. Within internal validity threats, 28% relate to instrumentation risks. Among prominent examples, we found a study in which the design assumes that a privacy-preserving eye gaze technique operates on a trusted platform, which ensures secure boot, integrity checks, and a protected open-source operating system (David-John et al., 2021). Another study introduces a type of malware that targets mixed reality headsets, operating under the assumption that it cannot modify the victim application because performing such an attack is highly complex (Luo et al., 2022). Although adopting this assumption can simplify the threat model, it might not precisely reflect the genuine capabilities of attackers in the real world. However, they do not explicitly describe mitigation strategies. In addition, we identified 15% related to tests that arise when the evaluation setup influences participant behavior or when the test conditions do not accurately reflect real-world usage. For example, a study of Li discusses a side-channel attack that occurs during the charging process of VR devices (Li et al., 2024). However, the testing setup introduced a limitation: one of the devices (MetaQuest Pro) used a charging pad that prevents it from being used while charging, unlike the other devices in the study that charged via cable. We also found that 13% of the articles describe instrumentation risks related to selection of settings and participants. For example, a study by Denning selected participants from a convenience sample inviting participants from coffee shops (Denning et al., 2014). However, the authors acknowledge the importance of including participants from a wider range of public locations, including workplaces, playgrounds, gyms, and bars, in order to more effectively capture the diverse behaviors and social interactions that could impact the viewpoints of viewers. Another study introduces a virtual ATM environment to examine user authentication behavior (Mathis et al., 2022). Although the VR setting provided a practical and cost-effective solution, it could not fully replicate the complexities of ATM interactions in the real world, such as the presence of bystanders or the pressure of being in a public space, which may have affected how participants behaved.Interestingly, the study explicitly describes the use of realistic sound effects, which enhance the immersive experience of the virtual environment to mitigate the impact of the threat.

External Validity.. Threats to external validity represent 37% of all studies and often focus on issues related to the setting and selection of participants, the latter being the most frequently addressed in 21%. For example, a study by Miller uses a dataset constructed from 41 right-handed users out of a total of 46 participants to train a Siamese network algorithm, raising concerns about the generalizability of the results of the authenti-

[13] https://github.com/pupil-labs/pupil
[14] https://pupil-labs.com/

Table 5: The 25 public repositories of security and privacy tools that involve the use of the metaverse.

Paper Type	Ref.	Repo. URL	Artefact	Framework	Language	Star	Fork	License	Archive	First Commit	Last Update	Running (years)
Application	(Kim et al., 2023)	Erebus	AC,ED,EX	ARCore,Unity	C,C#,Java	3	2	MIT	No	30.05.2023	21.09.2023	0.3
	(Trimananda et al., 2022)	OVRSeen	AC,ED,EX	Unity,Unreal	Javascript,Python	17	4	GPL-3.0,MIT	No	28.09.2021	27.10.2023	2.1
	(Lehman et al., 2022)	MAR Security	AC,EX	-	HTML,Java	1	0	-	No	18.05.2020	03.03.2022	1.8
	(Gordon et al., 2021)	CEC_VR	AC,ED,EX	Unity,Steam VR	C#	0	0	MIT	No	14.11.2019	17.12.2020	1.1
	(Rovira et al., 2013)	Arena Web Core	AC,EX	Unity	HTML, Javascript	41	28	BSD-3.0-Clause	No	17.07.2019	20.12.2024	5.4
	(Bozkir et al., 2019)	HMD Eyes	AC,EX	Unity	C#,Python	154	64	LGPL-3.0	No	20.04.2016	22.11.2022	6.6
	(Sluganovic et al., 2017)	Holopair	AC,EX	MRToolkit,Unity	C#	1	2	MIT	No	28.01.2016	08.06.2017	1.4
	(Garae et al., 2017)	NZCSC	ED	-	PHP	0	0	-	No	30.07.2020	07.07.2021	0.9
	(Figueiredo et al., 2016)	Prepose	AC,EX	Kinect SDK	C#	50	26	MIT	Yes	22.04.2015	26.11.2015	0.6
	(Liebers et al., 2024)	HMD Logger	AC,ED,EX	SteamVR	Python	3	0	-	No	08.09.2023	08.09.2023	0
	(Nair et al., 2024)	XROR	EX	-	Python	5	2	BSD-3.0-Clause	No	12.04.2023	20.03.2024	0.9
	(Kyu et al., 2024)	EITPose	AC,ED,EX	-	Python	10	1	MIT	No	24.01.2024	09.06.2024	0.4
	(Guo et al., 2024)	Meta Detector	AC,ED,EX	-	Python	4	0	-	No	02.05.2023	30.05.2024	1.1
Evaluation	(Nair et al., 2023a)	MetaGuard	AC,EX	-	Javascript,Python	13	8	MIT	No	17.02.2021	14.05.2023	2.2
	(Torres et al., 2023)	Web3	AC,ED,EX	-	CSS,Javascript,Python	12	1	MIT	No	23.06.2023	08.08.2023	0.1
	(Kaplan et al., 2023)	TagApp	AC,EX	-	Assembly, C	0	0	-	No	26.01.2022	26.01.2022	0
	(Nair et al., 2023b)	MetaDataStudy	AC,ED,EX	Unity	C#,Python	0	0	MIT	No	30.05.2022	30.05.2022	0
	(Cheng et al., 2024)	AR UI Security	AC	MRToolkit,Unity	C#,Java	4	1	MIT	No	08.10.2023	18.11.2023	0.1
Model	(Hanisch et al., 2023)	PETs2023	ED	Kinect SDK	Python	0	0	-	No	14.06.2022	23.08.2022	0.2
	(Vondráček et al., 2023)	SlimIt	AC,ED,EX	Unity	C,Python	0	0	MIT	Yes	02.05.2011	27.06.2020	9.2
Technique	(Nair et al., 2023c)	MetaGuard	AC,EX	Unity	C#	17	2	MIT	No	24.04.2022	16.08.2022	0.3
	(Miller et al., 2022a)	VR Biometric[15]	AC,ED,EX	-	Python	8	2	-	No	08.06.2022	13.06.2022	0
	(Huang and Ling, 2022)	SPAA	AC,ED,EX	-	Python	9	3	Custom	No	30.04.2023	13.05.2023	0
	(Rack et al., 2024)	Motion	AC,ED,EX	Unity	Python	0	0	-	No	23.08.2024	10.10.2024	0.1
	(Kumar et al., 2024)	Fidel AsiaCCS	AC,ED,EX	-	Python	0	0	-	No	16.04.2024	04.07.2024	0.2

cation behavior obtained from the model (Miller et al., 2021). The threat is mitigated using the leave-one-out cross-validation strategy. In other words, one out of the 41 participants is reserved for testing, while the other 40 are utilized for training. This process is repeated 41 times, with a different user being excluded each time. If the results remain consistent across these iterations, it suggests that the findings of the model could be generalized.

Construct Validity.. We found 5% of the studies that describe threats to construct validity. For example, Zhao's user study asks participants to provide a self-reported evaluation of their personal sense of safety (Zhao et al., 2019). Although the study lacks details of the mitigation strategies used, the authors propose incorporating more objective techniques, including biometric indicators such as heart rate variability or skin conductance, in future research.

- Internal validity threats were the most prevalent, accounting for approximately 50% of all reported validity concerns, often due to flawed assumptions and unrealistic testing setups.
- External validity threats appeared in 37% of the studies, primarily due to non-representative participant samples, such as studies involving only right-handed users or limited device types.
- Construct and conclusion validity received minimal attention, with only 5% of the studies addressing construct validity and none discussing threats to conclusion validity.

Domain-Specific Differences. We note that validity threats are described in different ways depending on the domain (*i.e.*, security & privacy, software engineering, and human-computer interaction). In software engineering, threats to validity are generally addressed in a dedicated section, often located after the discussion of results and prior to the conclusions. Sometimes, threats are structured using popular classifications. In contrast, in the security & privacy and the human-computer interaction domains the discussion of threats to validity is scattered in the content of multiple sections (often concentrated in the discussion). In each domain, we identified a limited number of studies specifying mitigation strategies applied to alleviate potential validity threats. However, such mentions appear more frequently in software engineering research. We think that the lack of a designated section to elaborate on validity threats in the security and privacy domain might hinder the clear articulation of mitigation measures.

4. Threats to Validity

We discuss potential threats to the validity of our study and outline the mitigation strategies we implemented to address these threats. These threats are classified into threats to internal and external validity.

4.1. Threats to internal validity

Data collection: Our study relies on the accuracy of our data collection strategy. We conducted a systematic literature review, using keywords related to the metaverse and security/privacy fields to identify relevant articles. However, there may be some articles with pertinent content that we missed due to the absence of

specific keywords. To address this, we iteratively refined our search queries and cross-referenced them with venues listed in the Core Ranking (A*, A, and B categories). Furthermore, we excluded duplicates and secondary studies that did not include evaluations, allowing us to maintain our focus on relevant studies.

Classification Bias: Human bias in the categorization and analysis of articles can impact the study's findings. To address this, two authors independently extracted and classified the data, resolving any conflicts through consensus discussions. This approach helps minimize individual biases and ensures that classifications accurately reflect the content of included studies.

4.2. Threats to external validity

Generalizability of Results: Our study focused on articles published in select venues that address specific immersive technologies within the metaverse. As a result, our findings may not apply to all situations or areas of the metaverse, especially those not directly included in this study. To address this limitation, we incorporated a variety of publications in the fields of software engineering, security and privacy, and human-computer interaction. In addition, our analysis is based on the content of the studies. Since these studies were published in venues with rigorous peer review processes, we are confident in their credibility and accuracy.

5. Conclusion

We conducted a systematic review of security and privacy research in metaverse published between 2013 and 2024. We observed notable advancements in key areas such as authentication, confidentiality, and usability. However, significant gaps remain that require immediate attention from researchers and practitioners. Limited research on back-end infrastructure and network communication protocols, coupled with the absence of scalability assessments, raises questions about the robustness of current metaverse systems in large-scale real-world deployments. Similarly, minimal attention to interoperability introduces risks for cross-platform data exchange and integration, which are pivotal to fostering a cohesive metaverse ecosystem. The substantial focus on human participant-based evaluations underscores the importance of user-centric approaches; however, the lack of studies addressing accessibility for individuals with disabilities signifies an equity gap that could impede inclusive participation. Furthermore, regulatory and compliance considerations remain inadequately addressed, potentially leaving metaverse platforms vulnerable to privacy breaches and legal challenges.

To tackle these challenges, a more comprehensive and balanced research agenda is required, moving beyond isolated technical approaches toward integrated strategies that encompass usability, scalability, and ethical governance. As metaverse technologies evolve, there is an increasing need to deepen investigations into emerging areas such as AI-driven privacy-preserving mechanisms and adaptive load management that can enhance security without compromising performance or user experience. At the same time, establishing robust interoperability standards and transparent consent frameworks will be essential to build user trust across heterogeneous platforms. Taken together, these insights highlight that addressing the security and privacy challenges of the metaverse requires recognizing the deep interconnection between technical complexity and human experience, and advancing integrated interdisciplinary efforts to create immersive environments that are secure, inclusive and worthy of trust.

CRediT authorship contribution statement

Argianto Rahartomo: Writing – original draft, methodology, data curation, investigation, validation. **Leonel Merino:** Writing – review & editing, validation, supervision. **Mohammad Ghafari:** Writing – review & editing, validation, supervision.

Declaration of competing interest

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

Acknowledgment

Leonel Merino is funded by ANID FONDECYT Iniciación Folio 11230349.

Data availability

The full data set including the information of the studies, classifications, and extra figures are publicly available: https://doi.org/10.5281/zenodo.15738685.

References

Abraham, M., Mcgill, M., Khamis, M., 2024. What you experience is what we collect: User experience based fine-grained permissions for everyday augmented reality, in: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, Association for Computing Machinery, New York, NY, USA. pp. 1–24. URL: https://doi.org/10.1145/3613904.3642668, doi:10.1145/3613904.3642668.

ACM, 2021. Empirical Standards. URL: https://www2.sigsoft.org/EmpiricalStandards/form_generator/Checklist.html.

Adams, D., Bah, A., Barwulor, C., Musaby, N., Pitkin, K., Redmiles, E.M., 2018. Ethics emerging: the story of privacy and security perceptions in virtual reality, in: Symposium On Usable Privacy and Security, USENIX Association, Baltimore, MD. pp. 427–442. URL: https://www.usenix.org/conference/soups2018/presentation/adams.

Alghamdi, A., Alkinoon, A., Alghuried, A., Mohaisen, D., 2024. xr-droid: A benchmark dataset for ar/vr and security applications. IEEE Transactions on Dependable and Secure Computing , 1–13doi:10.1109/TDSC.2024.3440662.

Andrabi, S.J., Reiter, M.K., Sturton, C., 2015. Usability of augmented reality for revealing secret messages to users but not their devices, in: Symposium On Usable Privacy and Security, USENIX Association, Ottawa. pp. 89–102. URL: https://www.usenix.org/conference/soups2015/proceedings/presentation/andrabi.

Arafat, A.A., Guo, Z., Awad, A., 2021. VR-Spy: A side-channel attack on virtual key-logging in VR headsets, in: IEEE Conference on Virtual Reality and 3D User Interfaces (VR), IEEE, Lisboa, Portugal. pp. 564–572. URL: https://ieeexplore.ieee.org/document/9417659/, doi:10.1109/VR50410.2021.00081.

Bozkir, E., Geisler, D., Kasneci, E., 2019. Person independent, privacy preserving, and real time assessment of cognitive load using eye tracking in a virtual reality setup, in: IEEE Conference on Virtual Reality and 3D User Interfaces (VR), IEEE, Osaka, Japan. pp. 1834–1837. URL: https://ieeexplore.ieee.org/document/8797758/, doi:10.1109/VR.2019.8797758.

Caine, K., 2016. Local standards for sample size at chi, in: Proceedings of the 2016 CHI conference on human factors in computing systems, pp. 981–992.

Campbell, D.T., Cook, T.D., 1979. Quasi-experimentation - design and analysis issues for field settings. Chicago, IL: Rand Mc-Nally 1, 1–384. URL: https://toc.library.ethz.ch/objects/pdf_uzh50/5/978-0-395-30790-8_006226431.pdf.

Cao, J., B, A.S., Das, A., Emami-Naeini, P., 2024. Understanding parents' perceptions and practices toward children's security and privacy in virtual reality, in: 2024 IEEE Symposium on Security and Privacy (SP), pp. 1554–1572. doi:10.1109/SP54263.2024.00222.

Casey, P., Baggili, I., Yarramreddy, A., 2021. Immersive virtual reality attacks and the human joystick. IEEE Transactions on Dependable and Secure Computing 18, 550–562. URL: https://ieeexplore.ieee.org/document/8675340/, doi:10.1109/TDSC.2019.2907942.

Cheng, K., Bhattacharya, A., Lin, M., Lee, J., Kumar, A., Tian, J.F., Kohno, T., Roesner, F., 2024. When the user is inside the user interface: An empirical study of UI security properties in augmented reality, in: 33rd USENIX Security Symposium (USENIX Security 24), USENIX Association, Philadelphia, PA. pp. 2707–2723. URL: https://www.usenix.org/conference/usenixsecurity24/presentation/cheng-kaiming.

Cheng, K., Tian, J.F., Kohno, T., Roesner, F., 2023. Exploring user reactions and mental models towards perceptual manipulation attacks in mixed reality, in: USENIX Security Symposium, USENIX Association, Anaheim, CA. pp. 911–928. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/cheng-kaiming.

David-John, B., Hosfelt, D., Butler, K., Jain, E., 2021. A privacy-preserving approach to streaming eye-tracking data. IEEE Transactions on Visualization and Computer Graphics 27, 2555–2565. URL: https://ieeexplore.ieee.org/document/9382914/, doi:10.1109/TVCG.2021.3067787.

De Guzman, J.A., Thilakarathna, K., Seneviratne, A., 2019a. A first look into privacy leakage in 3d mixed reality data, in: Sako, K., Schneider, S., Ryan, P.Y.A. (Eds.), Computer Security – ESORICS. Springer International Publishing, Cham. volume 11735, pp. 149–169. URL: http://link.springer.com/10.1007/978-3-030-29959-0_8, doi:10.1007/978-3-030-29959-0_8. series Title: Lecture Notes in Computer Science.

De Guzman, J.A., Thilakarathna, K., Seneviratne, A., 2019b. Security and privacy approaches in mixed reality: A literature survey. ACM Computing Surveys 52. URL: https://doi.org/10.1145/3359626, doi:10.1145/3359626.

Deldari, E., Freed, D., Poveda, J., Yao, Y., 2023. An investigation of teenager experiences in social virtual reality from teenagers', parents', and bystanders' perspectives, in: Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023), USENIX Association, Anaheim, CA. pp. 1–17. URL: https://www.usenix.org/conference/soups2023/presentation/deldari.

Denning, T., Dehlawi, Z., Kohno, T., 2014. In situ with bystanders of augmented reality glasses: perspectives on recording and privacy-mediating technologies, in: CHI Conference on Human Factors in Computing Systems, ACM, Toronto Ontario Canada. pp. 2377–2386. URL: https://dl.acm.org/doi/10.1145/2556288.2557352, doi:10.1145/2556288.2557352.

DeVrio, N., Mollyn, V., Harrison, C., 2023. SmartPoser: Arm pose estimation with a smartphone and smartwatch using UWB and IMU data, in: ACM Symposium on User Interface Software and Technology, ACM, San Francisco CA USA. pp. 1–11. URL: https://dl.acm.org/doi/10.1145/3586183.3606821, doi:10.1145/3586183.3606821.

Dudley, J.J., Jacques, J.T., Kristensson, P.O., 2021. Crowdsourcing design guidance for contextual adaptation of text content in augmented reality, in: CHI Conference on Human Factors in Computing Systems, ACM, Yokohama Japan. pp. 1–14. URL: https://dl.acm.org/doi/10.1145/3411764.3445493, doi:10.1145/3411764.3445493.

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., Gupta, A., Hinsch, C., Jain, A., Jane Patel, N., Jung, T., Juneja, S., Kamran, Q., Mohamed AB, S., Pandey, N., Papagiannidis, S., Raman, R., Rauschnabel, P.A., Tak, P., Taylor, A., tom Dieck, M.C., Viglia, G., Wang, Y., Yan, M., 2023. Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse. Information Systems Frontiers 25, 2071–2114. URL: https://doi.org/10.1007/s10796-023-10400-x, doi:10.1007/s10796-023-10400-x.

Düzgün, R., Noah, N., Mayer, P., Das, S., Volkamer, M., 2022. SoK: A systematic literature review of knowledge-based authentication on augmented reality head-mounted displays, in: International Conference on Availability, Reliability and Security, ACM, Vienna Austria. pp. 1–12. URL: https://dl.acm.org/doi/10.1145/3538969.3539011, doi:10.1145/3538969.3539011.

Ens, B., Grossman, T., Anderson, F., Matejka, J., Fitzmaurice, G., 2015. Candid interaction: Revealing hidden mobile and wearable computing activities, in: ACM Symposium on User Interface

Software and Technology, ACM, Charlotte NC USA. pp. 467–476. URL: https://dl.acm.org/doi/10.1145/2807442.2807449, doi:10.1145/2807442.2807449.

Esen, F.S., Tinmaz, H., Singh, M. (Eds.), 2023. Metaverse: Technologies, Opportunities and Threats. volume 133 of *Studies in Big Data*. Springer Nature Singapore, Singapore. URL: https://link.springer.com/10.1007/978-981-99-4641-9, doi:10.1007/978-981-99-4641-9.

Farrukh, H., Mohamed, R., Nare, A., Bianchi, A., Celik, Z.B., 2023. LocIn: Inferring semantic location from spatial maps in mixed reality, in: USENIX Security Symposium, USENIX Association, Anaheim, CA. pp. 877–894. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/farrukh.

Figueiredo, L.S., Livshits, B., Molnar, D., Veanes, M., 2016. Prepose: Privacy, security, and reliability for gesture-based programming, in: IEEE Symposium on Security and Privacy (SP), IEEE, San Jose, CA. pp. 122–137. URL: http://ieeexplore.ieee.org/document/7546499/, doi:10.1109/SP.2016.16.

Gallardo, A., Choy, C., Juneja, J., Bozkir, E., Cobb, C., Bauer, L., Cranor, L., 2023. Speculative privacy concerns about AR glasses data collection. Privacy Enhancing Technologies 2023, 416–435. doi:https://doi.org/10.56553/popets-2023-0117.

Garae, J., Ko, R.K.L., Kho, J., Suwadi, S., Will, M.A., Apperley, M., 2017. Visualizing the new zealand cyber security challenge for attack behaviors, in: IEEE Trustcom/BigDataSE/ICESS, IEEE, Sydney, Australia. pp. 1123–1130. URL: http://ieeexplore.ieee.org/document/8029565/, doi:10.1109/Trustcom/BigDataSE/ICESS.2017.362.

George, C., Khamis, M., Buschek, D., Hussmann, H., 2019. Investigating the third dimension for authentication in immersive virtual reality and in the real world, in: IEEE Conference on Virtual Reality and 3D User Interfaces (VR), IEEE, Osaka, Japan. pp. 277–285. URL: https://ieeexplore.ieee.org/document/8797862/, doi:10.1109/VR.2019.8797862.

Gopal, S.R.K., Shukla, D., Wheelock, J.D., Saxena, N., 2023. Hidden reality: Caution, your hand gesture inputs in the immersive virtual world are visible to all!, in: USENIX Security Symposium, USENIX Association, Anaheim, CA. pp. 859–876. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/gopal.

Gordon, J.R., Curran, M.T., Chuang, J., Cheshire, C., 2021. Covert embodied choice: Decision-making and the limits of privacy under biometric surveillance, in: CHI Conference on Human Factors in Computing Systems, ACM, Yokohama Japan. pp. 1–12. URL: https://dl.acm.org/doi/10.1145/3411764.3445309, doi:10.1145/3411764.3445309.

Guo, H., Dai, H.N., Luo, X., Zheng, Z., Xu, G., He, F., 2024. An empirical study on oculus virtual reality applications: Security and privacy perspectives, in: Proceedings of the IEEE/ACM 46th International Conference on Software Engineering, Association for Computing Machinery, New York, NY, USA. pp. 1–13. URL: https://doi.org/10.1145/3597503.3639082, doi:10.1145/3597503.3639082.

Hadan, H., Wang, D.M., Nacke, L.E., Zhang-Kennedy, L., 2024. Privacy in immersive extended reality: Exploring user perceptions, concerns, and coping strategies, in: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, Association for Computing Machinery, New York, NY, USA. pp. 1–24. URL: https://doi.org/10.1145/3613904.3642104, doi:10.1145/3613904.3642104.

Hamici-Aubert, V., Saint-Martin, J., Navas, R.E., Papadopoulos, G.Z., Doyen, G., Lagrange, X., 2024. Leveraging overshadowing for time-delay attacks in 4g/5g cellular networks: An empirical assessment, in: Proceedings of the 19th International Conference on Availability, Reliability and Security, Association for Computing Machinery, New York, NY, USA. pp. 1–10. URL: https://doi.org/10.1145/3664476.3670891, doi:10.1145/3664476.3670891.

Hanisch, S., Muschter, E., Hatzipanayioti, A., Li, S.C., Strufe, T., 2023. Understanding person identification through gait. Privacy Enhancing Technologies 2023, 177–189. doi:https://doi.org/10.56553/popets-2023-0011.

Harborth, D., Frik, A., 2021. Evaluating and redefining smartphone permissions with contextualized justifications for mobile augmented reality apps, in: Symposium On Usable Privacy and Security, USENIX Association, USA. pp. 513–534. URL: https://www.usenix.org/conference/soups2021/presentation/harborth.

Hartl, A.D., Arth, C., Grubert, J., Schmalstieg, D., 2016. Efficient verification of holograms using mobile augmented reality. IEEE Transactions on Visualization and Computer Graphics 22, 1843–1851. URL: http://ieeexplore.ieee.org/document/7321828/, doi:10.1109/TVCG.2015.2498612.

Hasselbring, W., 2021. Benchmarking as empirical standard in software engineering research, in: International Conference on Evaluation and Assessment in Software Engineering, Association for Computing Machinery, New York, NY, USA. p. 365–372. URL: https://doi.org/10.1145/3463274.3463361, doi:10.1145/3463274.3463361.

Huang, B., Ling, H., 2022. SPAA: Stealthy projector-based adversarial attacks on deep image classifiers, in: IEEE Conference on Virtual Reality and 3D User Interfaces (VR), IEEE, Christchurch, New Zealand. pp. 534–542. URL: https://ieeexplore.ieee.org/document/9756739/, doi:10.1109/VR51125.2022.00073.

Huang, Y., Li, Y.J., Cai, Z., 2023. Security and privacy in metaverse: A comprehensive survey. Big Data Mining and Analytics 6, 234–247. doi:10.26599/BDMA.2022.9020047.

John, B., Jorg, S., Koppal, S., Jain, E., 2020. The security-utility trade-off for iris authentication and eye animation for social virtual avatars. IEEE Transactions on Visualization and Computer Graphics 26, 1880–1890. URL: https://ieeexplore.ieee.org/document/8998133/, doi:10.1109/TVCG.2020.2973052.

Kaplan, B., Lopez-Toledo, I.J., Gunter, C., Qian, J., 2023. A tagging solution to discover iot devices in apartments, in: Annual Computer Security Applications Conference, Association for Computing Machinery, New York, NY, USA. p. 205–215. URL: https://doi.org/10.1145/3627106.3627108, doi:10.1145/3627106.3627108.

Katins, C., Woźniak, P.W., Chen, A., Tumay, I., Le, L.V.T., Uschold, J., Kosch, T., 2024. Assessing user apprehensions about mixed reality artifacts and applications: The mixed reality concerns (mrc) questionnaire, in: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, Association for Computing Machinery, New York, NY, USA. pp. 1–13. URL: https://doi.org/10.1145/3613904.3642631, doi:10.1145/3613904.3642631.

Khan, H., Hengartner, U., Vogel, D., 2020. Mimicry attacks on smartphone keystroke authentication. ACM Transactions on Privacy and Security 23, 1–34. URL: https://dl.acm.org/doi/10.1145/3372420, doi:10.1145/3372420.

Kim, Y., Goutam, S., Rahmati, A., Kaufman, A., 2023. Erebus: Access control for augmented reality systems, in: USENIX Security Symposium, USENIX Association, Anaheim, CA. pp. 929–946. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/kim-yoonsang.

Kitchenham, B., Charters, S., Budgen, D., Brereton, P., Turner, M., Linkman, S., Jørgensen, M., Mendes, E., Visaggio, G., 2007. Guidelines for performing systematic literature reviews in software

engineering. Technical Report. Technical report, ver. 2.3 EBSE technical report. EBSE.

Kumar, A., Aguilera, M.A.G., Tourani, R., Misra, S., 2024. A generative framework for low-cost result validation of machine learning-as-a-service inference, in: Proceedings of the 19th ACM Asia Conference on Computer and Communications Security, Association for Computing Machinery, New York, NY, USA. p. 1246–1260. URL: https://doi.org/10.1145/3634737.3657015, doi:10.1145/3634737.3657015.

Kyu, A., Mao, H., Zhu, J., Goel, M., Ahuja, K., 2024. Eitpose: Wearable and practical electrical impedance tomography for continuous hand pose estimation, in: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, Association for Computing Machinery, New York, NY, USA. pp. 1–10. URL: https://doi.org/10.1145/3613904.3642663, doi:10.1145/3613904.3642663.

Lantz, P., Johansson, B., Hell, M., Smeets, B., 2015. Visual cryptography and obfuscation: A use-case for decrypting and deobfuscating information using augmented reality, in: Brenner, M., Christin, N., Johnson, B., Rohloff, K. (Eds.), Financial Cryptography and Data Security. Springer Berlin Heidelberg, Berlin, Heidelberg. volume 8976, pp. 261–273. URL: https://link.springer.com/10.1007/978-3-662-48051-9_19, doi:10.1007/978-3-662-48051-9_19. series Title: Lecture Notes in Computer Science.

Lebeck, K., Ruth, K., Kohno, T., Roesner, F., 2017. Securing augmented reality output, in: IEEE Symposium on Security and Privacy (SP), IEEE, San Jose, CA, USA. pp. 320–337. URL: http://ieeexplore.ieee.org/document/7958585/, doi:10.1109/SP.2017.13.

Lebeck, K., Ruth, K., Kohno, T., Roesner, F., 2018. Towards security and privacy for multi-user augmented reality: Foundations with end users, in: IEEE Symposium on Security and Privacy (SP), IEEE, San Francisco, CA. pp. 392–408. URL: https://ieeexplore.ieee.org/document/8418615/, doi:10.1109/SP.2018.00051.

Lee, H., Lee, J., Kim, D., Jana, S., Shin, I., Son, S., 2021. AdCube: WebVR ad fraud and practical confinement of third-party ads, in: USENIX Security Symposium, USENIX Association, virtual. pp. 2543–2560. URL: https://www.usenix.org/conference/usenixsecurity21/presentation/lee-hyunjoo.

Lehman, S.M., Alrumayh, A.S., Kolhe, K., Ling, H., Tan, C.C., 2022. Hidden in plain sight: Exploring privacy risks of mobile augmented reality applications. ACM Transactions on Privacy and Security 25, 1–35. URL: https://dl.acm.org/doi/10.1145/3524020, doi:10.1145/3524020.

Lehrbaum, V., MacWilliams, A., Newman, J., Sudharsan, N., Bien, S., Karas, K., Eghtebas, C., Weber, S., Klinker, G., 2022. Enabling customizable workflows for industrial AR applications, in: IEEE International Symposium on Mixed and Augmented Reality (ISMAR), IEEE, Singapore, Singapore. pp. 622–630. URL: https://ieeexplore.ieee.org/document/9995600/, doi:10.1109/ISMAR55827.2022.00079.

Li, J., Chowdhury, A.R., Fawaz, K., Kim, Y., 2021a. Kaleido: Real-time privacy control for eye-tracking systems, in: USENIX Security Symposium, USENIX Association, virtual. pp. 1793–1810. URL: https://www.usenix.org/conference/usenixsecurity21/presentation/li-jingjie.

Li, J., Meng, Y., Zhan, Y., Zhang, L., Zhu, H., 2024. Dangers behind charging vr devices: Hidden side channel attacks via charging cables. IEEE Transactions on Information Forensics and Security 19, 8892–8907. doi:10.1109/TIFS.2024.3465026.

Li, L., Chen, C., Pan, L., Zhang, L.Y., Zhang, J., Xiang, Y., 2023. SigA: rPPG-based authentication for virtual reality head-mounted display, in: International Symposium on Research in Attacks, Intrusions and Defenses, ACM, Hong Kong China. pp. 686–699. URL: https://dl.acm.org/doi/10.1145/3607199.3607209, doi:10.1145/3607199.3607209.

Li, T., Liu, Y., Ma, S., Hu, M., Liu, T., Song, W., 2022. NailRing: An intelligent ring for recognizing micro-gestures in mixed reality, in: IEEE International Symposium on Mixed and Augmented Reality (ISMAR), IEEE, Singapore, Singapore. pp. 178–186. URL: https://ieeexplore.ieee.org/document/9994985/, doi:10.1109/ISMAR55827.2022.00032.

Li, Y., Cheng, Y., Meng, W., Li, Y., Deng, R.H., 2021b. Designing leakage-resilient password entry on head-mounted smart wearable glass devices. IEEE Transactions on Information Forensics and Security 16, 307–321. URL: https://ieeexplore.ieee.org/document/9153060/, doi:10.1109/TIFS.2020.3013212.

Liebers, J., Abdelaziz, M., Mecke, L., Saad, A., Auda, J., Gruenefeld, U., Alt, F., Schneegass, S., 2021. Understanding user identification in virtual reality through behavioral biometrics and the effect of body normalization, in: CHI Conference on Human Factors in Computing Systems, ACM, Yokohama Japan. pp. 1–11. URL: https://dl.acm.org/doi/10.1145/3411764.3445528, doi:10.1145/3411764.3445528.

Liebers, J., Laskowski, P., Rademaker, F., Sabel, L., Hoppen, J., Gruenefeld, U., Schneegass, S., 2024. Kinetic signatures: A systematic investigation of movement-based user identification in virtual reality, in: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, Association for Computing Machinery, New York, NY, USA. pp. 1–19. URL: https://doi.org/10.1145/3613904.3642471, doi:10.1145/3613904.3642471.

Lin, J., Cronjé, J., Wienrich, C., Pauli, P., Latoschik, M.E., 2023. Visual indicators representing avatars' authenticity in social virtual reality and their impacts on perceived trustworthiness. IEEE Transactions on Visualization and Computer Graphics 29, 4589–4599. URL: https://ieeexplore.ieee.org/document/10269746/, doi:10.1109/TVCG.2023.3320234.

Liu, G., Sun, X., Li, Y., Li, H., Zhao, S., Guo, Z., 2023a. An Automatic Privacy-Aware Framework for Text Data in Online Social Network Based on a Multi-Deep Learning Model. International Journal of Intelligent Systems 2023, 1727285. URL: https://onlinelibrary.wiley.com/doi/abs/10.1155/2023/1727285, doi:10.1155/2023/1727285. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1155/2023/1727285.

Liu, H., Xue, H., Zhao, L., Chen, D., Peng, Z., Zhang, G., 2023b. MagLoc-AR: Magnetic-based localization for visual-free augmented reality in large-scale indoor environments. IEEE Transactions on Visualization and Computer Graphics 29, 4383–4393. URL: https://ieeexplore.ieee.org/document/10269042/, doi:10.1109/TVCG.2023.3321088.

Liu, J., He, Y., Xiao, C., Han, J., Ren, K., 2024. Time to think the security of wifi-based behavior recognition systems. IEEE Transactions on Dependable and Secure Computing 21, 449–462. doi:10.1109/TDSC.2023.3261328.

Lu, D., Deng, Y., Huang, D., 2021. Global feature analysis and comparative evaluation of freestyle in-air-handwriting passcode for user authentication, in: Annual Computer Security Applications Conference, ACM, Virtual Event USA. pp. 468–481. URL: https://dl.acm.org/doi/10.1145/3485832.3485906, doi:10.1145/3485832.3485906.

Luo, S., Hu, X., Yan, Z., 2022. Hologlogger: Keystroke inference on mixed reality head mounted displays, in: IEEE Conference on Virtual Reality and 3D User Interfaces (VR), IEEE, Christchurch, New Zealand. pp. 445–454. URL: https://ieeexplore.ieee.org/document/9756771/, doi:10.1109/VR51125.2022.00064.

Luo, S., Nguyen, A., Farooq, H., Sun, K., Yan, Z., 2024. Eavesdropping on Controller Acoustic Emanation for Keystroke Inference Attack in Virtual Reality, in: Proceedings 2024 Network and Distributed System Security Symposium, Internet Society, San Diego, CA, USA. URL: https://www.ndss-symposium.org/wp-content/uploads/2024-100-paper.pdf, doi:10.14722/ndss.2024.24100.

Luo, S., Nguyen, A., Song, C., Lin, F., Xu, W., Yan, Z., 2020. Oculock: Exploring human visual system for authentication in virtual reality head-mounted display, in: Network and Distributed System Security Symposium, Internet Society, San Diego, CA. URL: https://www.ndss-symposium.org/wp-content/uploads/2020/02/24079.pdf, doi:10.14722/ndss.2020.24079.

Maddali, H.T., Lazar, A., 2023. Understanding context to capture when reconstructing meaningful spaces for remote instruction and connecting in XR, in: CHI Conference on Human Factors in Computing Systems, ACM, Hamburg Germany. pp. 1–18. URL: https://dl.acm.org/doi/10.1145/3544548.3581243, doi:10.1145/3544548.3581243.

Mathis, F., O'Hagan, J., Khamis, M., Vaniea, K., 2022. Virtual reality observations: Using virtual reality to augment lab-based shoulder surfing research, in: IEEE Conference on Virtual Reality and 3D User Interfaces (VR), IEEE, Christchurch, New Zealand. pp. 291–300. URL: https://ieeexplore.ieee.org/document/9756826/, doi:10.1109/VR51125.2022.00048.

Mathis, F., Vaniea, K., Khamis, M., 2021. RepliCueAuth: Validating the use of a lab-based virtual reality setup for evaluating authentication systems, in: CHI Conference on Human Factors in Computing Systems, ACM, Yokohama Japan. pp. 1–18. URL: https://dl.acm.org/doi/10.1145/3411764.3445478, doi:10.1145/3411764.3445478.

Merino, L., Schwarzl, M., Kraus, M., Sedlmair, M., Schmalstieg, D., Weiskopf, D., 2020. Evaluating mixed and augmented reality: A systematic literature review (2009-2019), in: 2020 IEEE International Symposium on Mixed and Augmented Reality (ISMAR), pp. 438–451. doi:10.1109/ISMAR50242.2020.00069.

Meteriz-Yildiran, U., Yildiran, N.F., Awad, A., Mohaisen, D., 2022. A keylogging inference attack on air-tapping keyboards in virtual environments, in: IEEE Conference on Virtual Reality and 3D User Interfaces (VR), IEEE, Christchurch, New Zealand. pp. 765–774. URL: https://ieeexplore.ieee.org/document/9756766/, doi:10.1109/VR51125.2022.00098.

Milgram, P., Kishino, F., 1994. A taxonomy of mixed reality visual displays. IEICE TRANSACTIONS on Information and Systems 77, 1321–1329.

Miller, R., Banerjee, N.K., Banerjee, S., 2021. Using siamese neural networks to perform cross-system behavioral authentication in virtual reality, in: IEEE Conference on Virtual Reality and 3D User Interfaces (VR), IEEE, Lisboa, Portugal. pp. 140–149. URL: https://ieeexplore.ieee.org/document/9417775/, doi:10.1109/VR50410.2021.00035.

Miller, R., Banerjee, N.K., Banerjee, S., 2022a. Combining real-world constraints on user behavior with deep neural networks for virtual reality (VR) biometrics, in: IEEE Conference on Virtual Reality and 3D User Interfaces (VR), IEEE, Christchurch, New Zealand. pp. 409–418. URL: https://ieeexplore.ieee.org/document/9756791/, doi:10.1109/VR51125.2022.00060.

Miller, R., Banerjee, N.K., Banerjee, S., 2022b. Temporal effects in motion behavior for virtual reality (VR) biometrics, in: IEEE Conference on Virtual Reality and 3D User Interfaces (VR), IEEE, Christchurch, New Zealand. pp. 563–572. URL: https://ieeexplore.ieee.org/document/9756745/, doi:10.1109/VR51125.2022.00076.

Mollyn, V., Harrison, C., 2024. Egotouch: On-body touch input using ar/vr headset cameras, in: Proceedings of the 37th Annual ACM Symposium on User Interface Software and Technology, Association for Computing Machinery, New York, NY, USA. pp. 1–11. URL: https://doi.org/10.1145/3654777.3676455, doi:10.1145/3654777.3676455.

Munsinger, B., Beebe, N., Richardson, T., 2023. Virtual reality for improving cyber situational awareness in security operations centers. Computers & Security 132, 103368. URL: https://linkinghub.elsevier.com/retrieve/pii/S016740482300278X, doi:10.1016/j.cose.2023.103368.

Munzner, T., 2008. Process and Pitfalls in Writing Information Visualization Research Papers. Springer Berlin Heidelberg, Berlin, Heidelberg. chapter 3. pp. 134–153. URL: https://doi.org/10.1007/978-3-540-70956-5_6, doi:10.1007/978-3-540-70956-5_6.

Nair, V., Guo, W., Mattern, J., Wang, R., O'Brien, J.F., Rosenberg, L., Song, D., 2023a. Unique identification of 50,000+ virtual reality users from head & hand motion data, in: USENIX Security Symposium, USENIX Association, Anaheim, CA. pp. 895–910. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/nair-identification.

Nair, V., Guo, W., Wang, R., O'Brien, J.F., Rosenberg, L., Song, D., 2024. Berkeley open extended reality recordings 2023 (boxrr-23): 4.7 million motion capture recordings from 105,000 xr users. IEEE Transactions on Visualization and Computer Graphics 30, 2239–2246. doi:10.1109/TVCG.2024.3372087.

Nair, V., Munilla Garrido, G., Song, D., O'Brien, J., 2023b. Exploring the privacy risks of adversarial vr game design. Privacy Enhancing Technologies 2023, 238–256. URL: https://petsymposium.org/popets/2023/popets-2023-0108.php, doi:10.56553/popets-2023-0108.

Nair, V.C., Munilla-Garrido, G., Song, D., 2023c. Going incognito in the metaverse: Achieving theoretically optimal privacy-usability tradeoffs in VR, in: ACM Symposium on User Interface Software and Technology, ACM, San Francisco CA USA. pp. 1–16. URL: https://dl.acm.org/doi/10.1145/3586183.3606754, doi:10.1145/3586183.3606754.

Nguyen, A., Zhang, X., Yan, Z., 2024. Penetration vision through virtual reality headsets: Identifying 360-degree videos from head movements, in: 33rd USENIX Security Symposium (USENIX Security 24), USENIX Association, Philadelphia, PA. pp. 2779–2796. URL: https://www.usenix.org/conference/usenixsecurity24/presentation/nguyen.

Patan, R., M. Parizi, R., 2023. Securing data exchange in the convergence of metaverse and IoT applications, in: International Conference on Availability, Reliability and Security, ACM, Benevento Italy. pp. 1–8. URL: https://dl.acm.org/doi/10.1145/3600160.3605019, doi:10.1145/3600160.3605019.

Pereira, N., Rowe, A., Farb, M.W., Liang, I., Lu, E., Riebling, E., 2021. Arena: The augmented reality edge networking architecture, in: IEEE International Symposium on Mixed and Augmented Reality (ISMAR), IEEE, Bari, Italy. pp. 479–488. URL: https://ieeexplore.ieee.org/document/9583841/, doi:10.1109/ISMAR52148.2021.00065.

Pham, D.M., 2018. Human identification using neural network-based classification of periodic behaviors in virtual reality, in: IEEE Conference on Virtual Reality and 3D User Interfaces (VR), IEEE, Reutlingen. pp. 657–658. URL: https://ieeexplore.ieee.org/document/8446529/, doi:10.1109/VR.2018.8446529.

Pooyandeh, M., Han, K.J., Sohn, I., 2022. Cybersecurity in the ai-based metaverse: A survey. Applied Sciences 12. URL: https://www.mdpi.com/2076-3417/12/24/12993, doi:10.3390/app122412993.

Rack, C., Schach, L., Achter, F., Shehada, Y., Lin, J., Latoschik, M.E., 2024. Motion passwords, in: Proceedings of the 30th ACM Symposium on Virtual Reality Software and Technology, Association for Computing Machinery, New York, NY, USA. pp. 1–11. URL: https://doi.org/10.1145/3641825.3687711, doi:10.1145/3641825.3687711.

Rahartomo, A., Merino, L., Ohshima, Y., Ghafari, M., 2025. The dilemma of privacy protection for developers in the metaverse, in: 2025 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), IEEE. pp. 284–290.

Rajaram, S., Chen, C., Roesner, F., Nebeling, M., 2023a. Eliciting security & privacy-informed sharing techniques for multi-user augmented reality, in: CHI Conference on Human Factors in Computing Systems, ACM, Hamburg Germany. pp. 1–17. URL: https://dl.acm.org/doi/10.1145/3544548.3581089, doi:10.1145/3544548.3581089.

Rajaram, S., Roesner, F., Nebeling, M., 2023b. Reframe: An augmented reality storyboarding tool for character-driven analysis of security & privacy concerns, in: ACM Symposium on User Interface Software and Technology, ACM, San Francisco CA USA. pp. 1–15. URL: https://dl.acm.org/doi/10.1145/3586183.3606750, doi:10.1145/3586183.3606750.

Ralph, P., 2021. Acm sigsoft empirical standards released. SIGSOFT Softw. Eng. Notes 46, 19. URL: https://doi.org/10.1145/3437479.3437483, doi:10.1145/3437479.3437483.

Riyadh, H.T.M.A., Bhardwaj, D., Dabrowski, A., Krombholz, K., 2024. Usable authentication in virtual reality: Exploring the usability of pins and gestures, in: Pöpper, C., Batina, L. (Eds.), Applied Cryptography and Network Security, Springer Nature Switzerland, Cham. pp. 412–431.

Roesner, F., Molnar, D., Moshchuk, A., Kohno, T., Wang, H.J., 2014. World-driven access control for continuous sensing, in: ACM SIGSAC Conference on Computer and Communications Security, ACM, Scottsdale Arizona USA. pp. 1169–1181. URL: https://dl.acm.org/doi/10.1145/2660267.2660319, doi:10.1145/2660267.2660319.

Rovira, A., Swapp, D., Southern, R., Zhang, J.J., Slater, M., 2013. The impact of enhanced projector display on the responses of people to a violent scenario in immersive virtual reality, in: IEEE Conference on Virtual Reality and 3D User Interfaces (VR), IEEE, Lake Buena Vista, FL. pp. 15–18. URL: http://ieeexplore.ieee.org/document/6549350/, doi:10.1109/VR.2013.6549350.

Ruth, K., Kohno, T., Roesner, F., 2019. Secure multi-user content sharing for augmented reality applications, in: USENIX Security Symposium, USENIX Association, Santa Clara, CA. pp. 141–158. URL: https://www.usenix.org/conference/usenixsecurity19/presentation/ruth.

Sabra, M., Vinayaga-Sureshkanth, N., Sharma, A., Maiti, A., Jadliwala, M., 2024. De-anonymizing vr avatars using non-vr motion side-channels, in: Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Association for Computing Machinery, New York, NY, USA. p. 54–65. URL: https://doi.org/10.1145/3643833.3656135, doi:10.1145/3643833.3656135.

Shen, Y., Wen, H., Luo, C., Xu, W., Zhang, T., Hu, W., Rus, D., 2019. Gaitlock: Protect virtual and augmented reality headsets using gait. IEEE Transactions on Dependable and Secure Computing 16, 484–497. URL: https://ieeexplore.ieee.org/document/8276563/, doi:10.1109/TDSC.2018.2800048.

Singha, A., Bi, Z., Li, T., Chen, Y., Zhang, Y., 2024. Securing contrastive mmwave-based human activity recognition against adversarial label flipping, in: Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Association for Computing Machinery, New York, NY, USA. p. 31–41. URL: https://doi.org/10.1145/3643833.3656123, doi:10.1145/3643833.3656123.

Slocum, C., Zhang, Y., Abu-Ghazaleh, N., Chen, J., 2023. Going through the motions: AR/VR keylogging from user head motions, in: USENIX Security Symposium, USENIX Association, Anaheim, CA. pp. 159–174. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/slocum.

Slocum, C., Zhang, Y., Shayegani, E., Zaree, P., Abu-Ghazaleh, N., Chen, J., 2024. That doesn't go there: Attacks on shared state in Multi-User augmented reality applications, in: 33rd USENIX Security Symposium (USENIX Security 24), USENIX Association, Philadelphia, PA. pp. 2761–2778. URL: https://www.usenix.org/conference/usenixsecurity24/presentation/slocum.

Sluganovic, I., Serbec, M., Derek, A., Martinovic, I., 2017. Holopair: Securing shared augmented reality using microsoft hololens, in: Annual Computer Security Applications Conference, ACM, Orlando FL USA. pp. 250–261. URL: https://dl.acm.org/doi/10.1145/3134600.3134625, doi:10.1145/3134600.3134625.

Smart, J., Cascio, J., Paffendorf, J., Bridges, C., Hummel, J., Hursthouse, J., Moss, R., 2007. A cross-industry public foresight project. Proc. Metaverse Roadmap Pathways 3DWeb , 1–28.

Stephenson, S., Pal, B., Fan, S., Fernandes, E., Zhao, Y., Chatterjee, R., 2022. SoK: Authentication in augmented and virtual reality, in: IEEE Symposium on Security and Privacy (SP), IEEE, San Francisco, CA, USA. pp. 267–284. URL: https://ieeexplore.ieee.org/document/9833742/, doi:10.1109/SP46214.2022.9833742.

Stone, S.A., Chapman, C.S., 2023. Unconscious frustration: Dynamically assessing user experience using eye and mouse tracking. Proc. ACM Hum.-Comput. Interact. 7. URL: https://doi.org/10.1145/3591137, doi:10.1145/3591137.

Sun, T., Ye, Y., Fujishiro, I., Ma, K.L., 2019. Collaborative visual analysis with multi-level information sharing using a wall-size display and see-through HMDs, in: IEEE Pacific Visualization Symposium (PacificVis), IEEE, Bangkok, Thailand. pp. 11–20. URL: https://ieeexplore.ieee.org/document/8781574/, doi:10.1109/PacificVis.2019.00010.

Sykownik, P., Maloney, D., Freeman, G., Masuch, M., 2022. Something personal from the metaverse: Goals, topics, and contextual factors of self-disclosure in commercial social VR, in: CHI Conference on Human Factors in Computing Systems, ACM, New Orleans LA USA. pp. 1–17. URL: https://dl.acm.org/doi/10.1145/3491102.3502008, doi:10.1145/3491102.3502008.

Torres, C.F., Willi, F., Shinde, S., 2023. Is your wallet snitching on you? an analysis on the privacy implications of web3, in: USENIX Security Symposium, USENIX Association, Anaheim, CA. pp. 769–786. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/torres.

Trimananda, R., Le, H., Cui, H., Ho, J.T., Shuba, A., Markopoulou, A., 2022. OVRseen: Auditing network traffic and privacy policies in oculus VR, in: USENIX Security Symposium, USENIX Association, Boston, MA. pp. 3789–3806. URL: https://www.usenix.org/conference/usenixsecurity22/presentation/trimananda.

Tseng, W.J., Bonnail, E., McGill, M., Khamis, M., Lecolinet, E., Huron, S., Gugenheimer, J., 2022. The dark side of perceptual manipulations in virtual reality, in: CHI Conference on Human Factors in Computing Systems, ACM, New Orleans LA USA. pp. 1–15. URL: https://dl.acm.org/doi/10.1145/3491102.3517728, doi:10.1145/3491102.3517728.

Vergari, M., Kojic, T., Vona, F., Garzotto, F., Moller, S., Voigt-Antons, J.N., 2021. Influence of interactivity and social environments on user experience and social acceptability in virtual reality,

in: IEEE Conference on Virtual Reality and 3D User Interfaces (VR), IEEE, Lisboa, Portugal. pp. 695–704. URL: https://ieeexplore.ieee.org/document/9417768/, doi:10.1109/VR50410.2021.00096.

Vilk, J., Molnar, D., Livshits, B., Ofek, E., Rossbach, C., Moshchuk, A., Wang, H.J., Gal, R., 2015. Surroundweb: Mitigating privacy concerns in a 3d web browser, in: IEEE Symposium on Security and Privacy, IEEE, San Jose, CA. pp. 431–446. URL: https://ieeexplore.ieee.org/document/7163040/, doi:10.1109/SP.2015.33.

Vo-Huu, T.D., Vo-Huu, T.D., Noubir, G., 2021. Spectrum-flexible secure broadcast ranging, in: ACM Conference on Security and Privacy in Wireless and Mobile Networks, ACM, Abu Dhabi United Arab Emirates. pp. 300–310. URL: https://dl.acm.org/doi/10.1145/3448300.3467819, doi:10.1145/3448300.3467819.

Vondráček, M., Baggili, I., Casey, P., Mekni, M., 2023. Rise of the metaverse's immersive virtual reality malware and the man-in-the-room attack & defenses. Computers & Security 127, 102923. URL: https://linkinghub.elsevier.com/retrieve/pii/S0167404822003157, doi:10.1016/j.cose.2022.102923.

Wan, T., Zhang, L., Xu, Y., Guo, Z., Gao, B., Liang, H.N., 2024. Analysis and design of efficient authentication techniques for password entry with the qwerty keyboard for vr environments. IEEE Transactions on Visualization and Computer Graphics 30, 7075–7085. doi:10.1109/TVCG.2024.3456195.

Wang, R., Huang, L., Wang, C., 2023. Low-effort VR headset user authentication using head-reverberated sounds with replay resistance, in: IEEE Symposium on Security and Privacy (SP), IEEE, San Francisco, CA, USA. pp. 3450–3465. URL: https://ieeexplore.ieee.org/document/10179367/, doi:10.1109/SP46215.2023.10179367.

Wilkowska, W., Offermann, J., Colonna, L., Florez-Revuelta, F., Climent-Pérez, P., Mihailidis, A., Poli, A., Spinsante, S., Ziefle, M., 2023. Interdisciplinary perspectives on privacy awareness in lifelogging technology development. Journal of Ambient Intelligence and Humanized Computing 14, 2291–2312. URL: https://doi.org/10.1007/s12652-022-04486-5, doi:10.1007/s12652-022-04486-5.

Wilson, E., Ibragimov, A., Proulx, M.J., Tetali, S.D., Butler, K., Jain, E., 2024. Privacy-preserving gaze data streaming in immersive interactive virtual reality: Robustness and user experience. IEEE Transactions on Visualization and Computer Graphics 30, 2257–2268. doi:10.1109/TVCG.2024.3372032.

Windl, M., Scheidle, A., George, C., Mayer, S., 2023. Investigating security indicators for hyperlinking within the metaverse, in: Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023), USENIX Association, Anaheim, CA. pp. 605–620. URL: https://www.usenix.org/conference/soups2023/presentation/windl.

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M.C., Regnell, B., Wesslén, A., 2024. Experimentation in Software Engineering. Springer, Berlin, Heidelberg. URL: https://link.springer.com/10.1007/978-3-662-69306-3, doi:10.1007/978-3-662-69306-3.

Wu, Y., Shi, C., Zhang, T., Walker, P., Liu, J., Saxena, N., Chen, Y., 2023. Privacy leakage via unrestricted motion-position sensors in the age of virtual reality: A study of snooping typed input on virtual keyboards, in: IEEE Symposium on Security and Privacy (SP), IEEE, San Francisco, CA, USA. pp. 3382–3398. URL: https://ieeexplore.ieee.org/document/10179301/, doi:10.1109/SP46215.2023.10179301.

Xu, W., Liang, H.N., Yu, K., Baghaei, N., 2021. Effect of gameplay uncertainty, display type, and age on virtual reality exergames, in: CHI Conference on Human Factors in Computing Systems, ACM, Yokohama Japan. pp. 1–14. URL: https://dl.acm.org/doi/10.1145/3411764.3445801, doi:10.1145/3411764.3445801.

Xu, Y., Price, T., Frahm, J.M., Monrose, F., 2016. Virtual u: Defeating face liveness detection by building virtual models from your public photos, in: USENIX Security Symposium, USENIX Association, Austin, TX. pp. 497–512. URL: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/xu.

Yadav, D.K., Ionascu, B., Krishna Ongole, S.V., Roy, A., Memon, N., 2015. Design and analysis of shoulder surfing resistant pin based authentication mechanisms on google glass, in: Brenner, M., Christin, N., Johnson, B., Rohloff, K. (Eds.), Financial Cryptography and Data Security. Springer Berlin Heidelberg, Berlin, Heidelberg. volume 8976, pp. 281–297. URL: https://link.springer.com/10.1007/978-3-662-48051-9_21, doi:10.1007/978-3-662-48051-9_21. series Title: Lecture Notes in Computer Science.

Yang, K., Zhang, Z., Youliang, T., Ma, J., 2023. A secure authentication framework to guarantee the traceability of avatars in metaverse. IEEE Transactions on Information Forensics and Security 18, 3817–3832. URL: https://ieeexplore.ieee.org/document/10159439/, doi:10.1109/TIFS.2023.3288689.

Yang, Z., Sarwar, Z., Hwang, I., Bhaskar, R., Zhao, B.Y., Zheng, H., 2024. Can virtual reality protect users from keystroke inference attacks?, in: 33rd USENIX Security Symposium (USENIX Security 24), USENIX Association, Philadelphia, PA. pp. 2725–2742. URL: https://www.usenix.org/conference/usenixsecurity24/presentation/yang-zhuolin.

Yu, H., Shokrnezhad, M., Taleb, T., Li, R., Song, J., 2023. Toward 6g-based metaverse: Supporting highly-dynamic deterministic multi-user extended reality services. IEEE Network 37, 30–38. doi:10.1109/MNET.004.2300101.

Zhang, K., Cochran, B.R., Chen, R., Hartung, L., Sprecher, B., Tredinnick, R., Ponto, K., Banerjee, S., Zhao, Y., 2024a. Exploring the design space of optical see-through ar head-mounted displays to support first responders in the field, in: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, Association for Computing Machinery, New York, NY, USA. pp. 1–19. URL: https://doi.org/10.1145/3613904.3642195, doi:10.1145/3613904.3642195.

Zhang, T., Ye, Z., Mahdad, A.T., Akanda, M.M.R.R., Shi, C., Wang, Y., Saxena, N., Chen, Y., 2023a. Facereader: Unobtrusively mining vital signs and vital sign embedded sensitive info via ar/vr motion sensors, in: ACM SIGSAC Conference on Computer and Communications Security, Association for Computing Machinery, New York, NY, USA. p. 446–459. URL: https://doi.org/10.1145/3576915.3623102, doi:10.1145/3576915.3623102.

Zhang, Y., Slocum, C., Chen, J., Abu-Ghazaleh, N., 2023b. It's all in your head(set): Side-channel attacks on AR/VR systems, in: USENIX Security Symposium, USENIX Association, Anaheim, CA. pp. 3979–3996. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/zhang-yicheng.

Zhang, Z., Yang, K., Tian, Y., Ma, J., 2024b. An anti-disguise authentication system using the first impression of avatar in metaverse. IEEE Transactions on Information Forensics and Security 19, 6393–6408. doi:10.1109/TIFS.2024.3410527.

Zhao, Y., Kupferstein, E., Castro, B.V., Feiner, S., Azenkot, S., 2019. Designing ar visualizations to facilitate stair navigation for people with low vision, in: ACM Symposium on User Interface Software and Technology, ACM, New Orleans LA USA. pp. 387–402. URL: https://dl.acm.org/doi/10.1145/3332165.3347906, doi:10.1145/3332165.3347906.

Zhu, H., Xiao, M., Sherman, D., Li, M., 2023. Soundlock: A novel user authentication scheme for VR devices using auditory-pupillary response, in: Network and Distributed System Security Symposium, Internet Society, San Diego, CA, USA. URL: https://www.ndss-symposium.org/wp-content/uploads/2023/02/ndss2023_f298_paper.pdf, doi:10.14722/ndss.2023.24298.

Argianto Rahartomo a Ph.D. candidate in the Secure Software Engineering (SSE) research group of TU Clausthal, Germany. He earned a Master of Science in Internet Technologies and Information Systems at Georg-August Universität Göttingen in Germany in 2017. His research interests include security and privacy in digital environments, with a focus on applications of gamification for security, privacy challenges in the metaverse, and spectrum management.

Leonel Merino is an Assistant Professor of Engineering Design in the School of Design and the School of Engineering at the Pontificia Universidad Católica de Chile, Santiago, Chile. His research interests include software engineering, information visualization, virtual and augmented reality, and human-computer interaction. He received a Ph.D. in Computer Science from the University of Bern and a M.Sc. in Computer Science from the E'cole des Mines de Nantes and the Vrije Universiteit Brussel. He is a member of the Steering Committee of VISSOFT and the IEEE Computer Society. Contact him at leonel.merino@uc.cl.

Mohammad Ghafari is a Professor of Software Engineering in TU Clausthal, where he leads the Secure Software Engineering (SSE) group. Mohammad's research focus is on developing tools and techniques that facilitate secure software development. He obtained his Ph.D. in Software Engineering from Politecnico di Milano in 2015. Contact him at mohammad.ghafari@tu-clausthal.de.