MASSXR 2025: The 3rd Workshop on Multi-modal Affective and Social Behavior Analysis and Synthesis in Extended Reality

(Affiliated with IEEE VR 2025)

Megha Quamara, Oya Celiktutan, Luca Viganò*
King's College London, UK

Aniket Bera†
Purdue University, IN, USA

Pablo Cesar‡
CWI and Delft University of Technology, The Netherlands

Funda Durupinar§
University of Massachusetts, Boston, MA, USA

Aline Normoyle¶
Bryn Mawr College, PA, USA

Chirag Raman‖
Delft University of Technology, The Netherlands

Zerrin Yumak**
Utrecht University, The Netherlands

ABSTRACT

The objective of MASSXR 2025, the 3rd Workshop on Multi-modal Affective and Social Behavior Analysis and Synthesis in Extended Reality, was to bring together researchers and practitioners from fields including cybersecurity, human-computer interaction, computer graphics/animation, multi-modal machine learning, Artificial Intelligence (AI), data privacy, and socio-technical studies to discuss the state of security in Extended Reality (XR), as well as future directions and opportunities. Through this, it aimed to achieve adaptive, context-aware security measures that are both technically robust and aligned with user trust and understanding. The workshop provided an opportunity to foster collaborative research efforts and advance the state of secure social interactions within XR, setting a foundation for future innovations in the field.

Index Terms: Extended Reality, Social-technical interactions, Cybersecurity, Privacy, Trustworthiness.

1 AMBITION

As Extended Reality (XR) technologies continue to advance, they bring forth transformative opportunities to redefine human interaction, communication, and immersion across various domains such as education, healthcare, entertainment, and industry [1]. However, alongside these innovations, they also introduce pressing challenges that must be addressed to ensure their successful and ethical integration into society. XR systems collect vast amounts of sensitive data—from user behaviors and interactions to biometrics—creating unique risks related to data breaches, unauthorized access, and identity theft [2, 3]. Ensuring robust security measures is thus essential to protect users and maintain trust in XR environments. Considering this, the MASSXR 2025 workshop aimed to explore the intersection of XR technologies and socio-technical security, focusing on the challenges and advancements in building secure, privacy-conscious, and trustworthy XR systems. It aimed to cover both technical safeguards and how users interact with and perceive XR technologies in a social context.

The workshop focused on the following research questions:

- How can we generate and analyze affective and social behaviors in XR? What are the latest techniques in this area?
- What are the latest advancements in safeguarding XR systems against privacy breaches and security vulnerabilities? How can we improve detection and mitigation strategies for reliable user protection?
- What are the current best practices for responsibly collecting, managing, and securing user interaction data within XR environments? How can data security be balanced with personalized experiences, and what privacy-aware innovations (e.g., for privacy-sensitive data recording, compression, or other management techniques) are emerging to support this?
- How can we enhance trust in XR applications through transparent data practices and robust identity management? What roles do authentication protocols, encryption, and user control mechanisms play in establishing trustworthy systems?
- What approaches (e.g., tools, techniques, methodologies) are emerging for providing secure, privacy-preserving, and resilient interactions in XR environments? How can Artificial Intelligence (AI)-based solutions support dynamic risk assessment and personalized security controls?
- How XR systems could be used to increase the security of other systems? What are the latest methods for using XR technologies in threat detection, authentication, and real-time security monitoring?

To that end, MASSXR 2025 aimed to bring together researchers and practitioners from fields including cybersecurity, human-computer interaction, computer graphics/animation, multi-modal machine learning, AI, data privacy, and socio-technical studies to discuss the state of security in XR, future directions, and opportunities to improve system robustness and user trust. Particular emphasis was put on the integration of AI with XR for adaptive, context-aware security measures that are both technically robust and aligned with user trust and understanding, in the expectation that the workshop would foster collaborative efforts and advance the state of secure social interactions within XR, setting a foundation for future innovations in the field via innovative approaches, experimental results, and theoretical insights into the security, privacy, and trustworthiness of XR systems.

The workshop webpage can be found at the following URL: https://sites.google.com/view/massxrworkshop2025.

2 PRIOR WORKSHOPS

The MASSXR 2025 workshop is the 3rd in the series, with the first held online at IEEE VR 2023, drawing around 45 attendees,

*{megha.quamara, oya.celiktutan, luca.vigano}@kcl.ac.uk
†ab@cs.purdue.edu
‡p.s.cesar@cwi.nl
§funda.durupinarbabur@umb.edu
¶anormoyle@brynmawr.edu
‖c.a.raman@tudelft.nl
**z.yumak@uu.nl

and the second conducted in person at IEEE VR 2024, attracting approximately 50 participants.

3 Scope

The MASSXR 2025 workshop invited researchers to submit original, high-quality research, survey, or position papers related to multi-modal affective and social behavior analysis and synthesis in XR, extending the focus on security and privacy in these environments. Relevant topics included, but are not limited to:

- Security and trustworthy interaction design
- Cybersecurity threats in XR
- Privacy in XR environments
- Secure cross-platform and cross-device communication
- AI and machine learning for security in XR
- Trustworthy social interactions and user collaboration in XR
- Ethics and compliance for data collection in XR
- Applications of XR for security and privacy

4 Program

The MASSXR 2025 workshop was organized as a half-day and an in-person event.

Two research papers and two work-in-progress papers were accepted for presentation, as detailed below:

- *Security and Privacy for VR in Non-entertainment Sectors: A Practice-based Study of the Challenges, Strategies and Gaps*, Camille Sivelle, David Palma, and Katrien De Moor: This work-in-progress explores the security and privacy (S&P) concerns of development teams and organizations using Virtual Reality (VR) in non-entertainment sectors, along with their mitigation strategies. Through semi-structured interviews with seven industry practitioners and analysis against VR S&P threat classifications, the authors identified gaps in threat awareness and defense strategies.
- *The Dilemma of Privacy Protection for Developers in the Metaverse*, Argianto Rahartomo, Leonel Merino, Mohammad Ghafari, and Yoshiki Ohshima: The authors investigated developers' support and awareness in handling sensitive data in the metaverse by surveying developers, consulting legal frameworks, and analyzing API documentation. Their findings underscore the urgent need for transparent privacy definitions, clear identification of sensitive data, and the implementation of effective protection measures.
- *User Identification based on Conversational Gestures*, Aline Normoyle and Sophie Joerg: This study presents a proof of concept investigating how social gestures can be used for identification in social virtual reality spaces. Using a dataset of eleven speakers collected via motion capture, the authors trained a fully convolutional network with features emulating motion tracking in virtual reality systems.
- *Emotion Recognition in Interactive VR tasks and in 360VR Videos with Transformer-Based Approaches and Multimodal Sensing*, Bharat KC, Bhoj Bahadur Karki, Jason Wolfgang Woodworth, Adil Khokhar, and Christoph Borst Borst: This paper compares emotion recognition models trained on passive and active emotional stimuli, as Interactive Virtual Reality (VR) systems have been shown to elicit strong emotions. The authors present a study with a new dataset that induces emotion through both passive (VR videos) and active (interactive VR tasks) stimuli, training models on multiple input modalities (EEG, EDA, HR, pupil characteristics) using transformer and fully convolutional network-based deep learning architectures.

The workshop also featured two keynote speakers, each bringing complementary expertise to the event. Additionally, a dynamic panel discussion involving the keynote speakers, organizers, and audience members served as an interactive forum to examine the current state of the field, future directions, emerging opportunities, and significant challenges.

5 Organizing Committee

The MASSXR 2025 workshop was organized by: Megha Quamara, Oya Celiktutan, Luca Viganò, Aniket Bera, Pablo Cesar, Funda Durupinar, Aline Normoyle, Chirag Raman, Zerrin Yumak.

Acknowledgments

This workshop was partially supported by the Horizon Europe program under the Grant Agreement 101070351 ("SERMAS: Socially-acceptable eXtended Reality Models and Systems") and by Innovate UK.

References

[1] A. Alhakamy. Extended reality (xr) toward building immersive solutions: The key to unlocking industry 4.0. *ACM Computing Surveys*, 56(9):1–38, 2024. 1

[2] D. Cayir, A. Acar, R. Lazzeretti, M. Angelini, M. Conti, and S. Uluagac. Augmenting security and privacy in the virtual realm: An analysis of extended reality devices. *IEEE Security & Privacy*, 2023. 1

[3] C. Warin and D. Reinhardt. Vision: Usable privacy for xr in the era of the metaverse. In *Proceedings of the 2022 European Symposium on Usable Security*, pp. 111–116, 2022. 1