IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 25, Issue 5, Ser. 2 (Sept. – October. 2023), PP 58-59
www.iosrjournals.org

Role of Metaverse in Next-Generation Behavioral-Learning and Communication Technologies to address data privacy and potential problems

Dr. Asok Biswas
Professor and Head of the Department,
Journalism & Multimedia, CGC Jhanjeri
Mohali, Punjab, India

Abstract:
Metaverse will work through next-generation behavioral-learning technologies such as virtual reality (VR), augmented reality (AR), artificial intelligence (AI) and machine learning (ML) that collect large amounts of data, often based on a user's personal information. As a result privacy is threatened. Considering the current state of security and data protection regulations, and in the absence of robust cyber security infrastructure, using such technologies within the metaverse can pose a significant threat to data privacy. Especially while we still haven't answered many of the privacy issues we face in ordinary reality, are we able to deal with potential issues with virtual reality, the general thought on privacy is—I have nothing to hide. Which may be right in a way but with the way the world is changing we might need something to protect us for sure. The Metaverse will be the new battlefield to fight for our privacy.

Keywords: *cybersecurity; artificial intelligence; metaverse; cyberattack; metaworld*

I. Introduction:

Our data stack is already out and accessible to most companies. With Metaverse, users' data privacy can be affected in unimaginable ways. From cyber attacks designed to steal data to targeting AR/VR devices that can be potential gateways to malware attacks and breaches. Another potential way to affect user privacy is the unauthorized collection of many personal data including biometric data, brainwaves, health information, preferences, resulting in deep user insights. In Metaworld, hackers will have a safe haven as they can quickly deploy targeted attacks to steal personal information with virtual avatars that operate through virtual identities.

CHALLENGES

Metaverse brings new challenges in its vast virtual world where users may be exposed to privacy attacks such as disclosure of privacy by other platform users. Some of the major challenges will be behavior and communication, including privacy and security of users at sensitive levels.

(1) Sensors: Extended Reality (XR) technology presents unimaginable privacy and security threats. As these technologies are based on sensors to scan and monitor the user's environment. Such data collected may be intelligible to users, for example head-mounted displays (used to display the Metaverse) may collect biometric data such as head movements, Eye tracking etc. which is unclear to users. A worrying example would be vision patterns. Collecting perspective data can give away users' sexual preferences.

(2) Behavior and communication: Like biometric data, any social interactions like conversations with other avatars, feedback, etc. can tell users' mindsets. While these interactions may be valuable in predicting the habits, actions, and preferences of users in the metaverse, the possibility of putting the most personal aspects of our psyche at risk cannot be denied. Ownership, control and use of this data is the biggest question.

(3) Security of users: Apart from security, another major challenge is the protection of information collected while sharing and against tampering, which can affect security.

Preventive Measures Using Virtual Offices: Despite privacy and security concerns, companies are setting up virtual offices and we will contact Metaverse so certain preventive measures can be taken by companies such as: (a) Watertight data privacy and security policies governing personal The use of information should be implemented by the company setting up virtual offices. (b) Along with AR/VR devices deployed by companies, companies should closely monitor and enable security against cyber attacks, hack attacks, data breaches and adversary AI attacks.

RECOMMENDATIONS

Meta- Selling with a visual lifestyle of users increases the possibility of data collection because our companies can be its new data source and VR headsets can learn more than traditional screens. Data collected from the real world is used in Metaverse to provide immersive experiences. Thus, privacy and security concerns will be an integral part of the metaverse as people worry about user identities, coercive surveillance, and potential misuse of personal information.

WAY FORWARD

A globally consistent enforceable privacy standard is the need of the hour. Not just policies, but governments need to invest in the capacity to investigate and enforce these standards in a timely manner.

II. Conclusion:

Companies must adhere to strict principles guiding the development of augmented reality products, including (a) ethics, (b) privacy, (c) safety, and (d) security. The inevitable dependence on the metaverse creates a dire need for companies to implement privacy by design while organizations/companies developing technology and privacy in the metaverse need to be carefully considered and protected. An evolved personal data and privacy protection that will guarantee an individual's identity with property in the virtual world is the basic need. This will lead to a situation where users will be forced to share more personal data to identify themselves. This will require data protection protocols to evolve to a whole new level. In the absence of overall data protection controls, Indian government/regulators will face a challenging situation to keep personal data safe and ensure that security systems work efficiently. Especially when it comes to regulations to protect privacy in the metaverse. Looking at the current situation where tech giants/social media platforms skirt their own policies and terms, regulators will have a tough time enforcing the law. These policies will hinder the power that tech companies gain in the metaverse by destroying users' privacy to exploit market advantages.

Reference:

[1]. Schultz, D. E. 2005. Special Issue Editorial. The Journal of Advertising Winter: 6-7.

[2]. Schultz, D. E. and P. J. Kitchen. 2000. A Response to 'Theoretical Concept of Management Fashion?' Journalof Advertising Research 40, no. 5: 17-21.

[3]. Shavitt, S., P. Vargas and P. Lowrey. 2004. Exploring the Role of Memory for self-Selected Ad Experiences: Are Some Advertising Media Better Liked than Others? Psychology and Marketing 21, no. 12: 1011-1032.

[4]. Swain, W. N. 2004. Perceptions of IMC after a Decade of Development: Who's at the Wheel, and How Can WeMeasure Success? Journal of Advertising Research 44, no. 1: 46-65.

[5]. Tektas. N. and E. D. Alakavuk. 2003. Allocation Model: An Effective Tool to Develop Media Plans for Turkey.International Journal of Advertising 22: 333-348.

[6]. Tellis, G. J. 2005. Advertising's Role in Capitalist Markets: What do we know and where do we go from here? Journal of Advertising Research June, 162-170.

[7]. Vakrata, D. and Z. Ma. 2005. A Look at the Long Run Effectiveness of Multimedia Advertising and itsImplications for Budget Allocation Decisions. Journal of Advertising Research June, 241-254.

[8]. World Advertising Research Centre. World Ad Spend. http://www.warc.com/LandingPages/Data/Adspend/AdspendByCountry.asp

About the author:

Dr. Asok Biswas is a Professor, Head of the Department of Journalism & Multimedia in the Chandigarh Group of College-Jhanjeri, Mohali, Punjab. His research focuses on Media planning and buying, advertising, human behavior and media management, market research and survey.