Brain-Computer Interface Integration With Extended Reality (XR): Future, Privacy And Security Outlook

Tuomo Lahtinen[1], Andrei Costin[1] and Guillermo Suarez-Tangil[2]
[1]Faculty of Information Technology, University of Jyväskylä, Jyväskylä, Finland
[2]IMDEA Network Institute, Madrid, Spain

tutalaht@jyu.fi
ancostin@jyu.fi
guillermo.suarez-tangil@imdea.org

Abstract: The Brain-Computer Interface (BCI) is a rapidly evolving technology set to revolutionize our perception of the Internet of Things (IoT). BCI facilitates direct communication between the brain and external devices, enabling the control or interaction of devices without physical intervention. BCI technology is becoming more sophisticated, allowing third-party software embedded in emerging technologies such as Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR) to access sensors that read brain activity. These can be grouped under the umbrella term Extended Reality (XR). While BCI technology is disrupting the way data is collected, interpreted, and utilized within IoT networks, it is important to consider the potential privacy and security threats that it poses. Previous and not-so-recent cybersecurity research only scratched the surface in terms of security and privacy aspects of the then-emerging neural and brain-connecting technologies. However, recent advances in reconstructing language, music tracks, and imagery solely based on decoding neural signals pose a significant risk of mental privacy invasion and cybersecurity abuse. In this paper, we present an analysis of the potential threats posed by the integration of BCI with VR, AR, and MR. We analyze the involvement of major technological players in shaping BCI and XR advancements, examining the potential for these technologies to create detailed user profiles and reshape the monetization of user data in the ever-more-aggressive data-driven economy. We also outline a position view on the cybersecurity aspects that are not related to privacy and profiling per se, for example, cybersecurity attacks on the brain (e.g., ``brain rewriting'' attacks) facilitated by potentially vulnerable XR-BCI devices and software. The paper concludes by emphasizing the need for further research on the privacy and security implications of XR-BCI integration and inviting deeper exploration of the topic beyond theoretical papers and toward a more applied experimental setup.

Keywords: Brain-Computer Interface, Extended Reality, Privacy, Big Tech, Cybersecurity, Metaverse

1. Introduction

A Brain-Computer Interface (BCI) allows people to control various devices with their thoughts. A BCI records brainwaves and translates them into commands. Despite rapid development in recent years, BCIs are still incomplete for many applications, but recent research shows promising results. Scientists have been able to reconstruct speech (Tang et al. 2023), images (Benchetrit et al. 2023), and music tracks (Bellier et al. 2023) from brain data with encouraging accuracy. This implies that more profound insights are on the horizon as BCI expands its influence into Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR), all encompassed by the overarching term eXtended Reality (XR).

Major industry players such as Meta are investing heavily in the metaverse and BCI technologies. However, the expanding presence of BCI in broader markets raises privacy and security concerns. Governance and management lapses among tech giants pose significant risks, intertwining with worries about market dominance, monopolization, and corporate surveillance. As BCI potentially harvests valuable brain data for commercial ends, ethical questions loom large: are users genuinely consenting to this data collection?

Our research delves into the threats and challenges associated with XR and BCI, and the potential fusion of these technologies into XR-BCI. We also highlight the influence of Big Tech, big data, and artificial intelligence (AI). The interdependence of these technologies, particularly evident in the metaverse's development, generates vast data volumes as users engage, creating a complex web of technological vulnerabilities. We refer to the Internet of Brains (IoB) (Harris 2008, Ju & Shen 2012) as the recent development of brain-computer interfaces, where brain data is accessible via modern telecommunications, peer-to-peer modes, or more generally via the Internet.

2. The XR Landscape

The history of VR, AR, or MR research dates back to the 90s. There have been ups and downs along the way, but now XR is closer to mass adoption than ever before as Big Tech companies push efforts into device development. Abraham et al. (2022) emphasized the importance of standards for the privacy and security implications of XR. When Google Glasses were commercially released in 2013, they were criticized for the privacy concerns raised

by stealthy video recording (Brewster 2014). Smart glasses can be used easily and inconspicuously to capture sensitive data from the environment. Privacy and security concerns are not just for the users of the devices, but also the privacy of bystanders, as Pahi & Schroeder (2023) mentioned. Modern extended reality devices have improved since the day Google Glass was released. Multiple sensors make it easy to track, for example, the user's behavior, actions, and gaze, and devices can also monitor the environment and surroundings such as people, places, and objects (Abraham et al. 2022).

There are many commercial XR headsets released such as Apple Vision Pro (2024), PlayStation VR 2 (2023), Meta Quest 3 (2023), HTC Vive Pro 2 (2021), Meta Quest 2 (2020), Oculus Quest 1 (2019), Valve Index (2019), PlayStation VR (2016). For XR-BCIs, there are mainly devices for development and research purposes such as OpenBCI Galea and Wearable Sensing DSI-VR300. In addition, CTRL-labs (acquired by Meta) has developed a wristband that can read electromyography (EMG) or EEG signals from the user, which can be used with the XR headset to enhance the XR experience through gesture management.

2.1 XR Research

XR technology is shifting from specific gaming and industrial applications to mass adoption by Big Tech companies. In the U.S., privacy adoption is not keeping pace with XR development. The most promising approach to address privacy threats is privacy regulation (Pahi & Schroeder 2023). When Abraham et al. (2022) were conducting research by organizing meetings between 13 XR experts, they discovered that experts were unaware of what data was collected and how valuable it was. As Ariely & Berns (2010) and Pahi & Schroeder (2023) stated, data collection must be as transparent as possible. It is very concerning if device users or even experts are unaware of the privacy policy.

The visual implementation of XR is via headset display. The content of the display could violate privacy. For example, Roesner & Kohno (2021) have shown that there is a possibility of a leak of visual information from the XR headset display that could contain sensitive data. Sensitive data can affect not only users of the XR headset but also bystanders. Bystander privacy can be a challenging issue because a bystander is often unaware of the information being collected (O'Hagan et al. 2023, Pahi & Schroeder 2023). Bystander data could include sensitive information about private homes or addresses, personal images, a person's visit to a hospital, or other locations that could contain sensitive information about an individual. To mitigate bystander threats, XR technology could automatically use blurring/distortion techniques to hide sensitive information such as images or voices (Pahi & Schroeder 2023).

XR provides the ability to observe long-term data such as height, movement, and gaze, which can be obtained directly. Indirect data, which is more sensitive, can also be obtained, such as sexual preferences, emotions, or mental state (Abraham et al. 2022). Combining this personal biometric data with the data obtained from the display could make identity theft very easy (O'Hagan et al. 2023).

2.2 XR-BCI Research

Existing XR-BCI (or VR-BCI/AR-BCI) research focuses predominantly on healthcare solutions and there is no mention of privacy or security. Some research has mentioned XR-BCI as a future possibility e.g. Saad et al. (2019), Cattan et al. (2020), Roesner & Kohno (2021). A review of the privacy and security of the XR-BCI domain is not feasible, but we present XR-BCI through existing technologies and open views for the future of XR-BCI.

Reading people's minds is not a new research topic. Ariely & Berns (2010) questioned the ability to measure people's preferences using neuroimaging. This concern can be mitigated by transparency, but Meta's privacy policy (Meta 2023) does not give a clear view of how eye-tracking data is used, and the same could be true for brain data if XR-BCI devices are commercialized.

Although XR-BCIs are currently available mainly for research purposes, existing XR headsets (see Section 2) can be developed to support BCIs, e.g. to provide an immersive and realistic experience by controlling an application or game with the mind. First, Kim et al. (2021) developed a drone control application using a P300-based XR-BCI (DSI-VR300) and administered a questionnaire to the 20 research participants. All participants controlled the drone well and were satisfied with both environments used in the research. No differences were found between the VR and AR environments in terms of performance and experience. Secondly, we discovered two different VR-BCI games on Steam, BCI VR Horror Attraction: The Mad Trail and VR BCI Meditation. While there are currently only two XR-BCI games available on Steam, Cattan et al (2020) investigated suitable game types for the P300-based VR-BCI games and found that 50% of the games are suitable for XR-BCI. Technical improvements

can also boost the commercialization of XR-BCI, for example, 6G networks and Saad et al (2019) also mention that XR-BCI is capable of replacing smartphones.

A new technology enables new risks. The integration of the physical world creates a threat if companies are interested in the environment of the XR user. Companies could collect data about the environment and people, and possible device-to-device integration could be implanted to facilitate the XR experience (Roesner & Kohno 2021). Roesner & Kohno (2021) also emphasize the importance of further research about interfacing with the brain and body to mitigate possible risks. These risks are created through sophisticated XR-BCI or other body-sensing technology. This technology could influence a person's thoughts, memories, and even physiology.

3. BCI Security and Privacy

Both privacy and security are very important parts of BCIs. Privacy and security must be ensured by keeping the firmware/software updated and adding various anti-virus/malware detection programs or data traffic management to prevent unauthorized system use (Lahtinen & Costin 2023). As Landau et al. (2020) and O'Hagan et al. (2023) suggest, it is important to keep unauthorized people away from the BCIs, and authorized people should only have minimal privileges (Tabasum et al. 2018). This can be done by establishing access control policies, for example, by defining who has access to raw data (O'Hagan et al. 2023).

Attacks against the security of BCI devices pose a risk to user privacy. Attacks could include unauthorized access or traffic sniffing in the BCI network. Tarkhani et al. (2022) were able to successfully capture data using Man-in-the-Middle (MitM) where the Bluetooth device was acting as a headset. The problem was that authentication was insufficient between the devices. The captured data can contain sensitive brain data and this data could legitimately be used to diagnose Alzheimer's disease, possibly other diseases, or sensitive information about the BCI user. It is important to understand that data leakage can occur in any part of the BCI system (Landau et al. 2020).

Invasive BCIs have more serious threats than non-invasive ones. Pycroft et al. (2016) presented possible attacks on DBS BCI devices. The attacks included severe attacks on the user's health, such as changing the stimulation frequency beyond a safe limit causing pain, affecting the user's emotions by stimulating inappropriate electrode contacts, or modulating reward processing. All the attacks presented are severe and their purpose is to change the user's emotions, and opinions or cause pain to the user. Brainjacking can be carried out by an attacker or person who wants to control someone's treatment, for example, parents who want to take over their daughter's treatment (Pugh et al. 2018).

For BCIs, Lahtinen & Costin (2023) propose adding "S" (Safety) into the well-known CIA (Confidentiality, Integrity, Availability) triad, essentially making it CIAS. If the BCI device can manage the current flow bidirectionally, it will expose the user to a health threat. BCI devices use WiFi or Bluetooth to communicate with the gateway device, and both technologies are vulnerable to MitM attacks where credentials are stolen and then used to gain unauthorized access to the BCI device (Lahtinen & Costin 2023). Once in control of the device, the attacker can perform various attacks (e.g. manipulate brain data or change stimulation frequency). The main threats that compromise safety are neural attacks (Bernal et al. 2023).

These privacy and security issues must be addressed when integrating the BCI with XR. XR-BCI may increase the total number of devices connected to the system, making access control and data transfer more difficult. Raw brain data can reveal sensitive information and a way to protect it is to encrypt brain data. If the BCI system is big, raw data could be hidden from some parts of the system, and access list/defining authorized persons who are allowed to see data is also important as Tabasum et al. (2018) suggested.

4. Enabling BCI Commercialization

The mainstream has not yet adopted BCIs because these devices are not affordable, the technology is not highly accurate enough, there are no complete commercially available solutions, etc. However, there has been good progress in creating new BCI devices in the name of reliability. Technologies are advancing and research is discovering ways to promote the commercialization of BCI.

This section presents these technologies and research to enable the commercialization of BCI. Most of the technologies/topics are interrelated and one could help to improve another. We present topics such as big tech, big data, metaverse, and AI in the light of XR-BCI development and commercialization.

4.1 Big Tech

The Big Tech companies are related to the BCIs through the development of the products and the acquisition of the BCI-related companies. The Big Tech companies also own and fund companies and researchers who are responsible for researching, developing, or selling AR, VR, and BCI devices. For example, Meta has its own research and development division, Reality Lab (Meta 2024), which focuses on extended reality, Microsoft is doing its research in the field of BCI (Microsoft 2024), and Elon Musk has founded Neuralink, which is developing invasive BCI to restore autonomy to people with medical conditions that limit daily life (Neuralink 2024). These companies have huge resources for BCI development and they can also acquire knowledge by acquiring other companies, such as Meta, acquired start-up CTRL-Labs, and VR-focused Oculus.

We also want to address the fact that Big Tech companies are also having a prominent impact in the areas of BCIs, AI, big data, etc. These companies are collecting huge amounts of data (e.g. user data) from engaged users and monetizing it in various ways. The amount of engaged users is the measure of power among Big Tech's (Birch et al. 2021).

4.2 Metaverse

The metaverse is a digital realm mirroring the physical world. Metaverse has been attracting attention for some years now and has also attracted the attention of the research community.

The key technology for the metaverse is XR, as it is an interactive technology for achieving an immersive experience (Chen et al. 2022). Immersion requires that the virtual world feels realistic enough to create an engrossing feeling both psychologically and emotionally, and BCI could enhance realism by triggering senses and feelings (Wang et al. 2022). XR headsets are also seen as a terminal for entering the metaverse.

The metaverse has received a lot of attention from researchers worldwide, but privacy and security have not been top priorities. Gupta et al. (2023) urge the implementation of privacy and security in metaverse design. These should be fundamental design elements, not add-ons (Gupta et al. 2023). A challenge in the metaverse is that if it incorporates multiple technologies, this could lead to a situation where known vulnerabilities and threats from the technologies are inherited into the metaverse (Wang et al. 2022).

The metaverse and the real world are connected, and what happens in the metaverse may affect the real world. For example, a security breach, denial-of-service, or identity theft in the metaverse could damage reputation and commerce in the real world. Common security and privacy challenges arising from technical features include privacy issues if the user anonymity model is the same as existing social networks. These issues include fake news, hate speech, online bullying, etc. (Gupta et al. 2023).

4.3 Big Data

The term big data was coined with the advent of digitalization. Big data is generated from online transactions, emails, media streams, search queries, health records, social networks, and mobile phones (Tene & Polonetsky 2012). This data asset exhibits substantial volume, velocity, and variety, necessitating the use of specific technologies and analytical methods to produce value (De Mauro et al. 2015).

When collecting big data, it is important to focus on the quality and reliability of the data. Poor quality data reduces the value of the data and creates threats and problems. From a business perspective, companies should have an interest in maintaining high-quality data, as poor quality is simply a waste of resources and monetizing would be challenging. Overall, the domain of big data privacy and security has four distinct areas: data management, data privacy, infrastructure security, integrity, and reactive security (Khanan et al. 2019).

Regulations and laws are important to bolster the privacy and security of big data. These vary from country to country, and some examples of regulations include GDPR (General Data Protection Regulation), the Privacy Act 1988 in Australia, and CCPA (California Consumer Privacy Act). However, the situation in the U.S. is not optimal as many of the proposed bills will not become law and only 11 of the 50 states have privacy laws(Folks 2024).

4.4 Artificial Intelligence

Artificial Intelligence is a growing field of technology that focuses on the development of intelligent machines. Machines that can act and behave like humans. Since the release of ChatGPT in November 2022, there has been a race to release AI platforms as everyone tries to push their own AI engine into the public domain. AI such as

ChatGPT can be seen as a tool to help BCI developers create devices. The benefits of using AI and LLMs (Large Language Models) (e.g., ChatGPT) are increased efficiency, accuracy, and cost savings (Deng & Lin 2022).

Many recent ChatGPT works (Aljanabi et al. 2023, Biswas 2023, Sakib et al. 2023, Surameery & Shakor 2023) suggest that it can be used to improve coding. ChatGPT understands natural language and this enables a user-friendly and more intuitive coding process. Coding and especially repeatable tasks are significantly accelerated when ChatGPT is used (Aljanabi et al. 2023, Surameery & Shakor 2023). As a tool, ChatGPT can be used to find and fix errors in the code (Roose 2022, Surameery & Shakor 2023) or to find security vulnerabilities (Aljanabi et al. 2023). Developers still need to have their skills as ChatGPT does not always provide working or the best solution to the problem. As with any answer ChatGPT provides, the answer to the coding problem depends entirely on the quality of the training data (Surameery & Shakor 2023).

The evolution of AI has the potential to boost BCI commercialization. Benchetrit et al. (2023) noted that generative and foundational AI systems have significantly improved the ability to decode brain activity in recent years. Their research used AI to create images by analyzing brain waves. Image detail is difficult to get right, but image categorization is reasonably good. AI could also improve and speed up patient diagnosis when applied to the analysis of BCI recordings. As neuroscience capabilities advance, this could help BCIs become more widely used in healthcare. On the other hand, AI could facilitate the development process for BCIs at the software level.

5. Discussion and Conclusion

We have discussed several technologies and methods that enable the commercialization of brain-computer interfaces (BCIs). In recent years, there have been significant advances in BCI research that have improved the technology's ability to generate accurate data. This data can be used to develop future commercial BCI devices. It should be noted that many BCI innovations and prototypes are not yet commercially available. However, using the technologies presented in Section 4, they are moving towards that goal.

Our research aims to provide insight into the future of advanced XR-BCI and BCI devices. Below, we discuss some of the key findings and conclusions.

The privacy and security challenges of XR are likely to increase when XR is integrated with BCI. Integration increases the field for cyber attackers and expands the sensitive data in the system, e.g. brain data. This is sensible when combining two technologies, the combination will inherit threats from both technologies, as suggested by Wang et al. (2022). The most valuable data for companies in terms of BCIs is brain data, which they can monetize to make a profit and, more worryingly, to profile and accurately identify individual users. The most effective way to protect brain data is through regulation (Pahi & Schroeder 2023), but, for example, U.S. Food and Drug Administration (FDA) approval of a device for medical use is not sufficient because it does not include rules on, for example, the collection of brain data for marketing purposes (Ariely & Berns 2010). Also, FDA approval does not remove the threat to the user's physical health if the device is maliciously programmed, e.g. neural attacks (Bernal et al. 2023), and with MitM it is possible to capture data between devices (Tarkhani et al. 2022).

Big Tech's push for more power creates privacy and security challenges. Privacy is not sufficiently considered when companies collect data for better user experience and device development. This could be the case, as Meta's privacy policy shows. Meta collects eye-tracking data, but only if the user chooses to enable eye-tracking features on the VR device. The eye-tracking data is collected and analyzed on the device and on Meta's servers, and some of the data may be stored for more personalized experiences and to improve Meta Quest (Meta's Eye Tracking Privacy Notice (2023)). The privacy notice does not explicitly reveal the data management's purpose but states that the data is collected and stored with the user's consent. This data could also be used for advertising purposes, as this 'personalized experience' suggests. The same could happen with the XR-BCI technology, with the company stating that it only collects data with the user's consent, but more importantly, that the user must provide it to enable the full functionality and experience of the device. We call this a hide-privacy-behind-feature, which is presented by Bryce (2019) as a medicine within a treat. As noted by Birch et al. (2021), when a user consents to data collection, they are entering into a contract with the company and giving up their legal right to use the data for monetization purposes. Privacy is not standard anymore but payable as an add-on known as pay-for-privacy (Bryce 2019).

The future of BCI devices sounds like science fiction when people can control computers with their minds. Control could extend to various devices, including the XR headset. Invasive BCI devices can record reasonably good quality brain data with a lot of potentially sensitive information that can be decoded in the future. IoB

opens up possibilities, but connecting the brain to the internet is an ambitious goal that could raise many concerns and ethical issues. Neuralink (Reuters 2023), Precision Neuroscience (Capoot 2023), and Synchron (Kelly 2023) have approval for human clinical trials and their devices can move forward quickly. For example, a Neuralink device is designed to control a computer, we see no barrier to controlling the XR device as well. While invasive BCIs for clinical use may take several years to be accepted in treatment, non-invasive BCIs could emerge much faster as they do not require approval, e.g. if non-invasive XR BCIs are used for entertainment purposes.

Although controlling computers, smart devices, games, etc. with one's brain (IoB) using AR/VR/XR devices combined with BCIs sounds great and may be considered cool, it is worth mentioning that there could be downsides. The questions are: how will BCI, XR, and XR-BCI manufacturers profit from developing devices, how will the user be engaged, and how will user data be monetized to generate revenue for the company? We see data leakage as the biggest threat to future XR-BCI devices. The human brain is a huge repository of information (e.g. credentials, knowledge, memories), identification (e.g. personality, values, emotions), non-repudiation, self-incrimination, and other sensitive and confidential bits. The implications of collecting and storing brain data, and improving data analysis methods in the future to extract more information from the data, can be devastating. Therefore additional deep and wide research efforts are required to ensure implicit privacy and security of BCI, and especially XR-BCI before they are mass-marketed.

Acknowledgments

Tuomo Lahtinen was supported by a grant from the Doctoral School, Faculty of Information Technology at the University of Jyväskylä.

G. Suarez-Tangil was supported by INCIBE's strategic project CIBERSEGURIDAD EINA UNIZAR, RYC-2020-029401-I, and TED2021-132900A-I00 funded by MCIN/AEI/10.13039/ 501100011033, NextGenerationEU/PRTR (Plan de Recuperación, Transformación y Resiliencia) and ESF.

References

Abraham, M., Saeghe, P., Mcgill, M. & Khamis, M. (2022), Implications of xr on privacy, security and behaviour: Insights from experts, in 'Nordic Human-Computer Interaction Conference'.

Aljanabi, M., Ghazi, M., Ali, A. H., Abed, S. A. et al. (2023), 'Chatgpt: open possibilities', Iraqi Journal For Computer Science and Mathematics.

Ariely, D. & Berns, G. S. (2010), 'Neuromarketing: the hope and hype of neuroimaging in business', Nature reviews neuroscience.

Bellier, L., Llorens, A., Marciano, D., Gunduz, A., Schalk, G., Brunner, P. & Knight, R. T. (2023), 'Music can be reconstructed from human auditory cortex activity using nonlinear decoding models', Public Library of Science PLoS biology.

Benchetrit, Y., Banville, H. & King, J.-R. (2023), 'Brain decoding: toward real-time reconstruction of visual perception', arXiv:2310.19812.

Bernal, S. L., Celdr´an, A. H. & P´erez, G. M. (2023), 'Eight reasons to prioritize brain-computer interface cybersecurity', Communications of the ACM.

Birch, K., Cochrane, D. & Ward, C. (2021), 'Data as asset? the measurement, governance, and valuation of digital personal data by big tech', Big Data & Society.

Biswas, S. (2023), 'Role of chatgpt in computer programming.: Chatgpt in computer programming.', Mesopotamian Journal of Computer Science.

Brewster, T. (2014), 'The many ways google glass users risk breaking british privacy laws'. [Accessed 16-01-2024].https://www.forbes.com/sites/thomasbrewster/2014/06/30/the-many-ways-google-glass-users-risk-breaking-british-privacy-laws/?sh=1c1648e747d8.

Bryce, C. (2019), 'Who invited the pay-for-privacy economy?'. [Accessed 20-01-2024]. https://medium.com/swlh/post-privacy-who-invited-the-pay-for-privacy-economy-626aecaf53e9.

Capoot, A. (2023), 'Neuralink competitor precision neuroscience conducts its first clinical study to map human brain signals'. [Accessed 22-01-2024]. https://www.cnbc.com/2023/06/23/precision-a-neuralink-competitor-conducts-its-first-clinical-study.html.

Cattan, G., Andreev, A. & Visinoni, E. (2020), 'Recommendations for integrating a p300-based brain–computer interface in virtual reality environments for gaming: An update', Computers.

Chen, Z., Wu, J., Gan, W. & Qi, Z. (2022), Metaverse security and privacy: An overview, in '2022 IEEE International Conference on Big Data (Big Data)', IEEE.

Costin, A., Zaddach, J., Francillon, A. & Balzarotti, D. (2014), A {Large-scale} analysis of the security of embedded firmwares, in '23rd USENIX security symposium'.

Costin, A., Zarras, A. & Francillon, A. (2016), Automated dynamic firmware analysis at scale: a case study on embedded web interfaces, in 'Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security'.

De Mauro, A., Greco, M. & Grimaldi, M. (2015), What is big data? a consensual definition and a review of key research topics, in 'AIP conference proceedings', American Institute of Physics.
Deng, J. & Lin, Y. (2022), 'The benefits and challenges of chatgpt: An overview', Frontiers in Computing and Intelligent Systems.
Folks, A. (2024), 'Us state privacy legislation tracker'. [Accessed 23-01-2024]. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/
Gupta, A., Khan, H. U., Nazir, S., Shafiq, M. & Shabaz, M. (2023), 'Metaverse security: Issues, challenges and a viable zta model', Electronics.
Harris, S. B. (2008), 'A million years of evolution', Year Million.
Ju, D. & Shen, B. (2012), 'Internet of knowledge plus knowledge cloud a future education ecosystem', Ieri Procedia.
Kelly, S. (2023), 'Synchron brain-computer interface implanted in first 6 us patients'. [Accessed 22-01-2024]. https://www.medtechdive.com/news/synchron-brain-computer-interface-implanted-first-patients/692843/.
Khanan, A., Abdullah, S., Mohamed, A. H. H. M., Mehmood, A. & Ariffin, K. A. Z. (2019), Big data security and privacy concerns: A review, in A. Al-Masri & K. Curran, eds, 'Smart Technologies and Innovation for a Sustainable Future', Springer International Publishing.
Kim, S., Lee, S., Kang, H., Kim, S., & Ahn, M. (2021). P300 brain–computer interface-based drone control in virtual and augmented reality. *Sensors*, *21*(17), 5765.
Lahtinen, T. & Costin, A. (2023), Linking computers to the brain: Overview of cybersecurity threats and possible solutions, in 'International Symposium on Business Modeling and Software Design', Springer.
Landau, O., Puzis, R. & Nissim, N. (2020), 'Mind your mind: Eeg-based brain-computer interfaces and their security in cyber space', ACM Computing Surveys (CSUR).
Meta (2023), 'Eye tracking privacy notice'. [Accessed 18-01-2024]. https://www.meta.com/en-gb/help/quest/articles/accounts/privacy-information-and-settings/eye-tracking-privacy-notice/.
Meta (2024), 'A future that's more human and less artificial'. [Accessed 24-01-2024]. https://about.meta.com/realitylabs/.
Microsoft (2024), 'Brain-computer interfaces'. [Accessed 05-01-2024]. https://www.microsoft.com/en-us/research/project/brain-computer-interfaces/overview/.
Neuralink (2024), 'Neuralink'. [Accessed 03-01-2024]. https://neuralink.com/.
O'Hagan, J., Saeghe, P., Gugenheimer, J., Medeiros, D., Marky, K., Khamis, M. & McGill, M. (2023), 'Privacy-enhancing technology and everyday augmented reality: Understanding bystanders' varying needs for awareness and consent', Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies.
Pahi, S. & Schroeder, C. (2023), 'Extended privacy for extended reality: Xr technology has 99 problems and privacy is several of them', Notre Dame J. on Emerging Tech.
Pugh, J., Pycroft, L., Sandberg, A., Aziz, T. & Savulescu, J. (2018), 'Brainjacking in deep brain stimulation and autonomy', Ethics and Information Technology.
Pycroft, L., Boccard, S. G., Owen, S. L., Stein, J. F., Fitzgerald, J. J., Green, A. L. & Aziz, T. Z. (2016), 'Brainjacking: implant security issues in invasive neuromodulation', World neurosurgery.
Reuters (2023), 'Musk's neuralink to start human trial of brain implant for paralysis patients'. [Accessed 22-01-2024].https://www.reuters.com/technology/musks-neuralink-start-human-trials-brain-implant-2023-09-19/.
Roesner, F. & Kohno, T. (2021), Security and privacy for augmented reality: Our 10-year retrospective, in 'VR4Sec: 1st International Workshop on Security for XR and XR for Security'.
Roose, K. (2022), 'The brilliance and weirdness of chatgpt', The New York Times.
Saad, W., Bennis, M. & Chen, M. (2019), 'A vision of 6g wireless systems: Applications, trends, technologies, and open research problems', IEEE network.
Sakib, F. A., Khan, S. H. & Karim, A. (2023), 'Extending the frontier of chatgpt: Code generation and debugging', arXiv:2307.08260.
Surameery, N. M. S. & Shakor, M. Y. (2023), 'Use chat gpt to solve programming bugs', International Journal of Information Technology & Computer Engineering (IJITC).
Tabasum, A., Safi, Z., AlKhater, W. & Shikfa, A. (2018), Cybersecurity issues in implanted medical devices, in '2018 International Conference on Computer and Applications (ICCA)', IEEE, pp. 1–9.
Tang, J., LeBel, A., Jain, S. & Huth, A. G. (2023), 'Semantic reconstruction of continuous language from non-invasive brain recordings', Nature Neuroscience.
Tarkhani, Z., Qendro, L., Brown, M. O., Hill, O., Mascolo, C. & Madhavapeddy, A. (2022), 'Enhancing the security & privacy of wearable brain-computer interfaces', arXiv preprint arXiv:2201.07711.
Tene, O. & Polonetsky, J. (2012), 'Big data for all: Privacy and user control in the age of analytics', Nw. J. Tech. & Intell. Prop.
Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H. & Shen, X. (2022), 'A survey on metaverse: Fundamentals, security, and privacy', IEEE Communications Surveys & Tutorials.