International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137

Volume – 08, Issue – 12, December 2023, PP – 77-84

Securing the Immersive Horizon: A Comprehensive Review of Secure 360 Video Streaming in Mixed Reality through Cloud Infrastructure

Koffka Khan[1]

[1]*Department of Computing and Information Technology (DCIT),*
The University of the West Indies, St. Augustine, Trinidad and Tobago

Abstract: This review paper provides a comprehensive exploration of secure 360-degree video streaming in the context of Mixed Reality (MR) within cloud environments. The integration of 360 video technology with MR applications has shown immense promise across various domains, necessitating a thorough investigation into the associated security challenges and potential solutions. The paper discusses the basics of 360 video technology and its applications in MR, emphasizing the significance of secure streaming. It delves into the security challenges specific to 360 video streaming in MR, addressing issues related to data privacy, content protection, and user authentication. The role of cloud infrastructure in supporting secure MR video streaming is examined, highlighting its significance in delivering scalable and efficient solutions. The review covers existing technologies, including encryption methods and access control mechanisms, designed to address security concerns. The paper also explores adaptive streaming techniques for delivering high-quality 360 videos in varying network conditions and discusses strategies for maintaining a consistent Quality of Service (QoS) while ensuring security. Additionally, the review anticipates potential advancements in secure 360 video streaming for MR, emphasizing the integration of emerging technologies such as artificial intelligence and blockchain. It identifies unresolved challenges in the domain, such as efficient content management and the need for standardized protocols. The paper concludes by emphasizing the importance of addressing security concerns for the continued growth of MR applications, providing potential directions for future research and development. The synthesis of findings underscores the need for a holistic approach to ensure the secure and immersive evolution of 360 MR video streaming within cloud environments.

Keywords: secure, 360-degree video streaming, Mixed Reality (MR), cloud

I. INTRODUCTION

The emerging field of Mixed Reality (MR) [20], [15], [2], [18] has witnessed a transformative integration of 360 video streaming, where users are immersed in dynamic and interactive environments blending the physical and virtual worlds. In this context, 360 video streaming introduces a novel dimension by capturing a complete panoramic view of the surroundings, providing users with an immersive and interactive experience. This technology allows users to explore virtual spaces as if they were physically present, making it particularly relevant for applications ranging from virtual tourism and education to collaborative workspaces.

As MR applications continue to evolve and gain traction, the significance of ensuring secure streaming becomes paramount. The immersive nature of 360 video in MR [22], [14], [24] introduces unique challenges related to data privacy, content protection, and user authentication. Unauthorized access to sensitive virtual environments or the interception of streaming data poses substantial risks. Therefore, securing the 360 video streaming in MR applications not only safeguards the integrity of the virtual experiences but also protects user data and privacy. Addressing these security concerns becomes essential to foster user trust, encourage broader adoption of MR technologies, and unlock the full potential of 360 video streaming in diverse industries.

Currently, the landscape of 360 video streaming and MR is intricately tied to cloud infrastructure. Cloud services play a pivotal role in supporting the storage, processing, and delivery of high-quality 360 video content to MR devices. Leveraging cloud resources enables scalable and efficient solutions for managing the complexity of 360 video streaming, ensuring seamless experiences for users. The integration of MR with cloud technologies has seen notable advancements, with various platforms offering frameworks and services tailored to the unique requirements of MR applications. Understanding the current state of 360 video streaming in MR within the cloud ecosystem is vital for comprehending the challenges and opportunities in implementing secure streaming solutions for these immersive experiences.

The paper, titled "Securing the Immersive Horizon: A Comprehensive Review of Secure 360 Video Streaming in Mixed Reality through Cloud Infrastructure," delves into the intricate landscape of secure 360

video streaming within the realm of Mixed Reality (MR) and its integration with cloud technologies. Beginning with an introduction to the significance of 360 video streaming in MR, the review explores the associated security challenges, encompassing issues of data privacy, content protection, and user authentication. A thorough examination of existing solutions and technologies follows, investigating encryption methods, access control mechanisms, and the role of cloud infrastructure in supporting scalable and secure MR video streaming. The paper also delves into critical aspects such as authentication, access control, data privacy, and adaptive streaming techniques, while foreseeing future trends and identifying challenges that warrant further research. The comprehensive review concludes by summarizing key findings and emphasizing the crucial need for addressing security concerns in the dynamic landscape of 360 video streaming for MR in the cloud.

II. BACKGROUND

360 video technology [21] a variant of traditional video streaming [6], [7], [8], [9] captures a complete spherical view of the surroundings, allowing users to immerse themselves in a panoramic experience. This immersive content is created using specialized cameras equipped with multiple lenses to capture a 360-degree perspective. In Mixed Reality (MR), 360 video becomes a powerful tool, as it seamlessly integrates with virtual environments, providing users with an enhanced sense of presence and interaction. In MR applications, users can not only view these 360-degree videos but also interact with virtual elements overlaid on the real-world environment. This blending of physical and virtual worlds enhances the overall user experience[4], [5], [11], making 360 video an integral component of MR applications in various domains, such as gaming, education, training, and virtual tourism.

Despite the immersive potential, streaming 360 videos in the context of MR presents several challenges. The sheer volume of data associated with 360-degree videos, which capture a vast field of view, poses significant bandwidth and storage challenges. Delivering high-quality streaming experiences requires overcoming issues related to latency, ensuring that the content is rendered seamlessly and without interruptions. Moreover, synchronizing the real-world environment with virtual overlays in MR adds complexity to the streaming process. Ensuring smooth transitions between the physical and virtual elements demands efficient data processing and delivery mechanisms. These challenges underscore the need for robust streaming solutions that not only address the technical aspects of data transmission but also cater to the immersive and interactive nature of MR experiences.

Cloud computing [12] plays a crucial role in supporting MR applications, including secure 360 video streaming. Cloud infrastructure provides scalable and flexible resources for storing, processing, and delivering 360 video content. With the ability to dynamically allocate resources based on demand, cloud platforms enable efficient handling of the computational requirements associated with streaming high-resolution 360 videos. Additionally, cloud services offer the necessary storage capacity to manage the vast amounts of data generated by 360-degree videos. The distributed nature of cloud computing contributes to low-latency delivery, enhancing the overall streaming experience for MR users. Leveraging cloud resources, MR applications can achieve scalability, reliability, and cost-effectiveness, making cloud computing an indispensable component in the ecosystem of secure 360 video streaming for Mixed Reality.

III. SECURITY CHALLENGES IN 360 VIDEO STREAMING FOR MR

Secure 360 Mixed Reality (MR) video streaming [17], [25], [3], [1] in the cloud introduces a set of unique security challenges that necessitate careful consideration and robust solutions. One prominent challenge lies in ensuring the confidentiality and integrity of the immersive content during the streaming process. The expansive field of view captured by 360-degree videos increases the risk of unauthorized access to sensitive virtual environments, potentially compromising the privacy of users and the confidentiality of the content being streamed. To address this, encryption techniques must be adeptly employed to protect the streaming data from interception or tampering. This involves encrypting the video content during transmission and implementing secure key management systems to control access to the encrypted data.

Data privacy emerges as a critical concern in the context of 360 video streaming in MR environments. The immersive nature of MR experiences, coupled with the potential for capturing real-world surroundings, necessitates stringent measures to protect user privacy. Issues may arise regarding the unintentional collection of personally identifiable information (PII) or the exposure of sensitive details within the captured content. An effective approach involves implementing privacy-preserving mechanisms, such as anonymization and pseudonymization, to mitigate the risks associated with data privacy breaches. Additionally, careful consideration must be given to user consent mechanisms, informing users about data collection practices and ensuring their explicit agreement.

Content protection is another crucial facet of securing 360 video streaming in MR environments. Unauthorized distribution, reproduction, or modification of immersive content poses significant threats. Digital rights management (DRM) solutions play a pivotal role in safeguarding the intellectual property embedded in 360-degree videos. These mechanisms control access to the content, preventing unauthorized duplication or redistribution. Additionally, watermarking techniques can be employed to trace the origin of content and deter potential infringements.

User authentication is paramount in ensuring that only authorized individuals can access and interact within MR environments. The immersive and interactive nature of 360 video in MR necessitates robust user authentication mechanisms to prevent unauthorized users from entering virtual spaces. Multi-factor authentication and biometric authentication methods can enhance the security of MR experiences by adding layers of verification beyond traditional username-password combinations. Implementing secure authentication practices is fundamental in establishing a trustworthy and protected environment for users engaging in 360 video streaming within the realm of Mixed Reality.

IV. EXISTING SOLUTIONS AND TECHNOLOGIES

A comprehensive review of existing technologies and solutions reveals a range of strategies employed to address security concerns in the domain of 360 Mixed Reality (MR) video streaming within cloud environments. Encryption methods stand out as a foundational component of secure streaming, ensuring that the transmitted 360 video data remains confidential and unaltered during transit. Advanced encryption algorithms, such as AES (Advanced Encryption Standard), are commonly used to secure the video streams. By encrypting the content, unauthorized parties are prevented from gaining access to the sensitive information within the 360 videos. Additionally, secure key management practices are implemented to control and authenticate access to the decryption keys, adding an extra layer of protection against unauthorized viewing or tampering.

Access control mechanisms play a vital role in defining and regulating user permissions within MR environments. Role-based access control (RBAC) systems, for instance, are instrumental in specifying the actions and operations that different user roles are authorized to perform. This helps prevent unauthorized individuals from manipulating or viewing certain aspects of the 360 video content [19]. Additionally, attribute-based access control (ABAC) provides a more dynamic approach, allowing access decisions based on various attributes such as user characteristics, environmental conditions, or specific contextual factors. By incorporating these access control measures, secure 360 video streaming ensures that only authenticated and authorized users have the appropriate level of access to MR content.

Beyond encryption and access control, other security measures contribute to a holistic approach in safeguarding 360 video streaming in MR environments. These may include secure transmission protocols (e.g., HTTPS), which protect against data interception during transit, and regular security audits to identify and rectify vulnerabilities. Continuous monitoring of user activities and anomaly detection mechanisms further enhance the security posture, enabling the identification of suspicious behavior that may indicate potential security threats. By combining encryption methods, access controls, and a suite of other security measures, the existing technologies in this field aim to create a robust and resilient framework for secure 360 video streaming in Mixed Reality environments hosted on cloud infrastructure.

V. CLOUD INFRASTRUCTURE FOR MR VIDEO STREAMING

The role of cloud infrastructure in supporting secure Mixed Reality (MR) video streaming, particularly in the context of 360-degree content, is integral to the seamless delivery and immersive experiences provided to users [16]. Cloud computing offers a scalable and flexible environment that effectively addresses the computational demands and storage requirements associated with 360 video streaming. The dynamic nature of MR applications, coupled with the large data volumes generated by 360-degree videos, necessitates a robust and scalable infrastructure. Cloud platforms provide the capability to dynamically allocate resources based on demand, ensuring optimal performance during peak usage periods and efficiently scaling down during periods of lower demand. This scalability is crucial for handling the intricacies of streaming high-quality 360 video content to MR devices.

Cloud-based solutions play a pivotal role in optimizing the efficiency of 360 video streaming in MR. Content delivery networks (CDNs) hosted on cloud platforms enhance the distribution of 360-degree videos by strategically placing content in multiple geographic locations. This reduces latency and accelerates the delivery of content to end-users, ensuring a smoother and more responsive MR experience. Additionally, cloud-based transcoding services enable the adaptation of video streams to different device specifications and network conditions, facilitating adaptive streaming. Adaptive streaming techniques dynamically adjust the quality of the video based on the viewer's device capabilities and network bandwidth, resulting in an optimized viewing

experience. Cloud infrastructure thus serves as a foundational element in creating a scalable, efficient, and responsive ecosystem for secure 360 video streaming in Mixed Reality.

VI. AUTHENTICATION AND ACCESS CONTROL

Ensuring secure user authentication in Mixed Reality (MR) environments is crucial for maintaining the integrity and confidentiality of 360-degree video streaming within the cloud [17], [19]. Various methods are employed to authenticate users, especially given the immersive and interactive nature of MR experiences. Multi-factor authentication (MFA) is a prominent approach, requiring users to provide multiple forms of identification, such as a password combined with a one-time verification code sent to their mobile device. This additional layer of authentication enhances security by making it more challenging for unauthorized users to gain access to MR environments. Biometric authentication, utilizing features like fingerprint or facial recognition, is another cutting-edge method that not only enhances security but also aligns with the seamless and natural interactions within MR spaces.

In conjunction with user authentication, robust access control mechanisms are essential to prevent unauthorized access to 360-degree video content. Role-Based Access Control (RBAC) assigns specific roles and permissions to users based on their responsibilities within the MR environment. For example, content creators may have different access rights compared to general viewers. Attribute-Based Access Control (ABAC) provides a more granular approach, allowing access decisions based on various attributes such as user characteristics or contextual factors. These mechanisms ensure that only authorized users with the appropriate roles and permissions can interact with and view specific aspects of the 360 video content. By implementing secure user authentication and access control measures, the overall security posture of MR environments is significantly strengthened, mitigating the risk of unauthorized access and potential misuse of 360-degree video content.

VII. DATA PRIVACY AND ENCRYPTION

Preserving data privacy is a paramount consideration in the realm of secure 360 Mixed Reality (MR) video streaming within cloud environments [26], [23], [13]. The immersive and interactive nature of MR experiences, coupled with the potential for capturing real-world surroundings in 360-degree videos, emphasizes the need for robust measures to protect user data and sensitive content. The importance of data privacy lies not only in complying with regulations but also in establishing trust with users who engage in MR video streaming. Users expect their personal information and the content they interact with to be handled with the utmost confidentiality and integrity.

Encryption techniques play a pivotal role in safeguarding both content and user data throughout the streaming process. To protect the confidentiality of 360-degree video content, end-to-end encryption is often employed. This involves encrypting the video data at the source, maintaining the encryption throughout transmission, and decrypting it only at the authorized destination. This ensures that even if the data is intercepted during transit, it remains indecipherable without the appropriate decryption keys. Additionally, user data, including personally identifiable information (PII) and authentication credentials, is subject to encryption. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols are commonly used to encrypt data transmitted between users and cloud servers, safeguarding it from potential eavesdropping or unauthorized access.

Implementing encryption techniques not only addresses the immediate need for data privacy but also contributes to building a secure foundation for MR video streaming in the cloud. By adopting robust encryption measures, the integrity and confidentiality of both the immersive content and user data are upheld, fostering a secure and trustworthy environment for individuals engaging in 360-degree video experiences within the dynamic landscape of Mixed Reality.

VIII. ADAPTIVE STREAMING AND QUALITY OF SERVICE (QOS)

Adaptive streaming techniques[6], [7], [8] play a pivotal role in ensuring the optimal delivery of high-quality 360-degree videos within varying network conditions in the context of secure Mixed Reality (MR) video streaming in the cloud. The immersive nature of MR experiences, combined with the intricate details of 360-degree video content, necessitates adaptive streaming to accommodate diverse network bandwidths and user devices. Adaptive streaming dynamically adjusts the quality of the video being delivered based on real-time network conditions, ensuring a seamless and uninterrupted viewing experience for users. This is particularly crucial in MR, where users navigate virtual environments while interacting with 360-degree content. Adaptive streaming protocols, such as Dynamic Adaptive Streaming over HTTP (DASH) or HTTP Live Streaming (HLS), segment the video content into smaller chunks of varying quality levels. The player then intelligently

selects and loads the appropriate segments based on the user's network speed and device capabilities, optimizing the viewing experience.

Maintaining a consistent Quality of Service (QoS) is essential in MR video streaming, and this becomes even more challenging when ensuring security concurrently. To achieve this balance, strategies involve a multifaceted approach. Firstly, the encryption and decryption processes must be efficiently managed to minimize any potential impact on QoS. Utilizing optimized encryption algorithms and key management systems ensures that the security measures do not compromise the speed and efficiency of data transmission. Additionally, implementing content delivery networks (CDNs) and edge computing services within the cloud infrastructure can enhance QoS by reducing latency and improving the responsiveness of MR applications. Regular monitoring and performance tuning are vital to identifying potential bottlenecks and optimizing the overall QoS without compromising on the security aspects of 360 video streaming. By integrating adaptive streaming techniques with thoughtful strategies for QoS maintenance, secure 360 MR video streaming in the cloud can deliver a high-quality and immersive experience to users under diverse network conditions.

IX. FUTURE TRENDS AND EMERGING TECHNOLOGIES

Potential advancements in secure 360 Mixed Reality (MR) video streaming within cloud environments are poised to reshape the landscape, offering enhanced user experiences and addressing evolving security challenges. One key area of advancement involves the integration of cutting-edge artificial intelligence (AI) technologies. AI-driven algorithms can play a pivotal role in content analysis, allowing for real-time identification of potential security threats, such as unauthorized access or suspicious activities within MR environments. Additionally, AI can contribute to adaptive streaming by dynamically optimizing the delivery of 360-degree videos based on user preferences, behaviors, and network conditions. By harnessing the power of machine learning [10], secure 360 video streaming can become more proactive and responsive, mitigating security risks while optimizing the immersive experience for users.

The exploration of blockchain technology [27] represents another promising avenue for advancing security in 360 MR video streaming. Blockchain's decentralized and tamper-resistant nature can enhance data integrity and authentication mechanisms. By employing blockchain for content verification and user identity management, the security of 360-degree videos can be fortified, ensuring the authenticity and traceability of the content throughout the streaming process. Smart contracts within blockchain frameworks may further automate secure transactions and access control, offering a decentralized solution to some of the current security challenges. As research in this field progresses, the fusion of blockchain technology with 360 MR video streaming holds the potential to establish a more transparent, secure, and accountable ecosystem.

Furthermore, the integration of advanced biometric authentication methods, such as gaze tracking and facial recognition, represents an emerging research direction in securing MR video streaming. These biometric markers can add an extra layer of user authentication, enhancing the overall security posture of MR environments. Exploring the fusion of biometrics with encryption and access control mechanisms can create a robust and user-friendly security framework, aligning with the natural interactions and immersion levels in MR experiences. As researchers delve deeper into these potential advancements and emerging technologies, the secure 360 video streaming landscape for MR is poised to evolve, offering a more sophisticated and resilient platform for immersive content delivery within the cloud.

X. CHALLENGES AND OPEN ISSUES

While significant strides have been made in the secure 360 Mixed Reality (MR) video streaming domain, several unresolved challenges and open issues persist, necessitating further research and development efforts. One prominent challenge is the efficient management of large-scale immersive content within the cloud. As 360-degree videos generate substantial data volumes, there is a need for innovative storage solutions, content delivery mechanisms, and data processing techniques that can handle the intricacies of MR streaming at scale. Balancing the demand for high-quality visuals and low-latency streaming with the constraints of available network bandwidth remains an ongoing challenge, particularly in scenarios where users engage with dynamic and interactive MR environments.

Another critical area requiring attention is the enhancement of security measures to keep pace with evolving threats. As technology advances, so do the tactics of potential adversaries seeking to compromise data integrity and user privacy. Continual research is needed to identify and address emerging security vulnerabilities, especially in the context of user authentication and content protection. Additionally, the intersection of security and privacy concerns raises complex ethical considerations, warranting interdisciplinary research to establish guidelines and frameworks that strike a balance between user protection and immersive content experiences.

Furthermore, the interoperability and standardization of secure 360 video streaming protocols for MR applications represent an area that requires concerted research efforts. Establishing industry standards will promote compatibility, allowing seamless integration across different platforms, devices, and cloud services. This standardization can contribute to a more cohesive ecosystem, facilitating broader adoption of secure 360 video streaming in MR.

In conclusion, the unresolved challenges and open issues in secure 360 MR video streaming underscore the need for ongoing research and development. Addressing these challenges will not only fortify the security and efficiency of immersive content delivery but also contribute to the broader advancement and adoption of Mixed Reality technologies within cloud environments.

In summarizing the key findings from the comprehensive review of secure 360 Mixed Reality (MR) video streaming in the cloud, several crucial insights emerge. The immersive integration of 360-degree video streaming with MR applications holds immense potential across various domains, including virtual tourism, education, and collaborative workspaces. However, this synergy introduces unique security challenges, ranging from data privacy concerns to the protection of sensitive content and the need for secure user authentication. The review underscores the critical role of cloud infrastructure in supporting scalable and efficient 360 video streaming, providing dynamic resources for storage, processing, and delivery.

The emphasis on security measures, including encryption techniques, access control mechanisms, and advanced authentication methods, resonates throughout the findings. These security protocols are essential for preserving data privacy, ensuring content protection, and safeguarding user interactions within MR environments. The exploration of adaptive streaming techniques and the integration of emerging technologies such as AI and blockchain further contribute to the evolution of secure 360 MR video streaming, enhancing both the quality of user experiences and the resilience of the underlying infrastructure.

The overarching message is clear: addressing security concerns is paramount for the successful advancement and widespread adoption of 360 video streaming in MR within cloud environments. User trust and confidence in the security of immersive experiences are pivotal for the continued growth of MR applications. As the technology landscape evolves, it becomes imperative for researchers, developers, and industry stakeholders to collaboratively address the identified challenges, foster innovation in security solutions, and establish best practices. By prioritizing security in the design and implementation of 360 MR video streaming, we can create a foundation for a trustworthy and immersive digital future.

XI. CONCLUSION

Looking ahead, the landscape of secure 360 Mixed Reality (MR) video streaming in the cloud presents exciting opportunities for future research and development. One promising avenue is the exploration of novel encryption techniques that can seamlessly balance security and computational efficiency. Research in this direction can lead to the development of encryption algorithms specifically tailored for the unique requirements of 360-degree video streaming, ensuring robust data protection without compromising real-time streaming performance. Additionally, advancements in homomorphic encryption or secure multi-party computation may offer innovative approaches to secure content delivery in MR environments, further enhancing the privacy and confidentiality of immersive experiences.

The integration of edge computing with cloud infrastructure is another area ripe for exploration. By distributing computational processes closer to the end-users in MR applications, edge computing can significantly reduce latency and enhance the responsiveness of streaming content. Future research can delve into optimizing the collaboration between cloud and edge computing resources to create a seamless and secure ecosystem for 360 video streaming. This exploration may involve the development of intelligent algorithms that dynamically allocate tasks between the cloud and edge nodes based on real-time network conditions and user interactions.

Moreover, the ethical implications of 360 MR video streaming, particularly in terms of user privacy and data usage, require in-depth examination. Future research should address questions surrounding the responsible collection, storage, and processing of user data within MR environments. Establishing ethical frameworks and guidelines for developers and service providers will be crucial to foster a transparent and trustworthy relationship with users.

Lastly, the standardization of protocols for secure 360 MR video streaming is a key area for future development. Establishing industry-wide standards will promote interoperability, facilitate collaboration, and ensure a consistent security posture across diverse platforms and devices. This standardization effort can contribute to a more cohesive and accessible ecosystem for 360 video streaming in MR, fostering innovation and broadening the scope of immersive experiences across various applications and industries.

REFERENCES

[1] Aslam AM, Chaudhary R, Bhardwaj A, Budhiraja I, Kumar N, Zeadally S. Metaverse for 6G and Beyond: the next revolution and deployMentChallenGes. IEEE Internet of Things Magazine. 2023 Mar 14;6(1):32-9.

[2] Buhalis D, Karatay N. Mixed reality (MR) for generation Z in cultural heritage tourism towards metaverse. InInformation and Communication Technologies in Tourism 2022: Proceedings of the ENTER 2022 eTourism Conference, January 11–14, 2022 2022 (pp. 16-27). Springer International Publishing.

[3] Jing A, May K, Matthews B, Lee G, Billinghurst M. The Impact of Sharing Gaze Behaviours in Collaborative Mixed Reality. Proceedings of the ACM on Human-Computer Interaction. 2022 Nov 11;6(CSCW2):1-27.

[4] Khan K, Goodridge W. QoE evaluation of dynamic adaptive streaming over HTTP (DASH) with promising transport layer protocols: Transport layer protocol performance over HTTP/2 DASH. CCF Transactions on Networking. 2020 Dec;3(3-4):245-60.

[5] Khan K, Goodridge W. QoE Evaluation of Legacy TCP Variants over DASH. International Journal of Advanced Networking and Applications. 2021 Mar 1;12(5):4656-67.

[6] Khan K, Goodridge W. Reinforcement Learning in DASH. International Journal of Advanced Networking and Applications. 2020 Mar 1;11(5):4386-92.

[7] Khan K, Goodridge W. SAND and Cloud-based Strategies for Adaptive Video Streaming. International Journal of Advanced Networking and Applications. 2017 Nov 1;9(3):3400-10.

[8] Khan K, Goodridge W. Variants of the Constrained Bottleneck LAN Edge Link in Household Networks. International Journal of Advanced Networking and Applications. 2019 Mar 1;10(5):4035-44.

[9] Khan K, Goodridge W. What happens when adaptive video streaming players compete in time-varying bandwidth conditions?. International journal of advanced networking and applications. 2018 Jul 1;10(1):3704-12.

[10] Khan K, Sahai A. A comparison of BA, GA, PSO, BP and LM for training feed forward neural networks in e-learning context. International Journal of Intelligent Systems and Applications. 2012 Jun 1;4(7):23.

[11] Koffka K, Wayne G. A DASH Survey: the ON-OFF Traffic Problem and Contemporary Solutions. Computer Sciences and Telecommunications. 2018(1):3-20.

[12] Mourtzis D, Angelopoulos J, Panopoulos N. Integration of Mixed Reality to CFD in Industry 4.0: A Manufacturing Design Paradigm. Procedia CIRP. 2022 Jan 1;107:1144-9.

[13] Murala DK, Panda SK. The Role of Immersive Reality (AR/VR/MR/XR) in Metaverse. Metaverse and Immersive Technologies: An Introduction to Industrial, Business and Social Applications. 2023 Oct 20:159-89.

[14] Piumsomboon T, Lee GA, Irlitti A, Ens B, Thomas BH, Billinghurst M. On the shoulder of the giant: A multi-scale mixed reality collaboration with 360 video sharing and tangible interaction. InProceedings of the 2019 CHI conference on human factors in computing systems 2019 May 2 (pp. 1-17).

[15] Rokhsaritalemi S, Sadeghi-Niaraki A, Choi SM. A review on mixed reality: Current trends, challenges and prospects. Applied Sciences. 2020 Jan 16;10(2):636.

[16] Siripurapu S, Darimireddy NK, Chehri A, AV P. Technological Advancements and Elucidation Gadgets for Healthcare Applications: An Exhaustive Methodological Review-Part-II (Robotics, Drones, 3D-Printing, Internet of Things, Virtual/Augmented and Mixed Reality). Electronics. 2023 Jan 20;12(3):548.

[17] Skaggs-Schellenberg R, Wright D, Tayeb S. A Secure Mixed Reality Framework for the Internet of Things. InProceedings of the Future Technologies Conference (FTC) 2021, Volume 3 2022 (pp. 387-396). Springer International Publishing.

[18] Speicher M, Hall BD, Nebeling M. What is mixed reality?.InProceedings of the 2019 CHI conference on human factors in computing systems 2019 May 2 (pp. 1-15).

[19] Szczurek KA, Prades RM, Matheson E, Rodriguez-Nogueira J, Di Castro M. Multimodal multi-user mixed reality human–robot interface for remote operations in hazardous environments. IEEE Access. 2023 Feb 15;11:17305-33.

[20] Tang YM, Au KM, Lau HC, Ho GT, Wu CH. Evaluating the effectiveness of learning design with mixed reality (MR) in higher education. Virtual Reality. 2020 Dec;24(4):797-807.

[21] Violante MG, Vezzetti E, Piazzolla P. Interactive virtual technologies in engineering education: Why not 360° videos?. International Journal on Interactive Design and Manufacturing (IJIDeM). 2019 Jun 1;13(2):729-42.

[22] Wang P, Bai X, Billinghurst M, Zhang S, Zhang X, Wang S, He W, Yan Y, Ji H. AR/MR remote collaboration on physical tasks: a review. Robotics and Computer-Integrated Manufacturing. 2021 Dec 1; 72:102071.

[23] Worlikar H, Coleman S, Kelly J, O'Connor S, Murray A, McVeigh T, Doran J, McCabe I, O'Keeffe D. Mixed Reality Platforms in Telehealth Delivery: Scoping Review. JMIR Biomedical Engineering. 2023 Mar 24; 8:e42709.

[24] Xu M, Li C, Zhang S, Le Callet P. State-of-the-art in 360 video/image processing: Perception, assessment and compression. IEEE Journal of Selected Topics in Signal Processing. 2020 Jan 15;14(1):5-26.

[25] Yun WG, Youn JK, Ko D, Yeom I, Joo HJ, Kong HJ, Kim HY. Tele-consent using mixed reality glasses (NREAL) in pediatric inguinal herniorrhaphy: a preliminary study. Scientific Reports. 2022 Feb 24;12(1):3105.

[26] Yun WG, Youn JK, Ko D, Yeom I, Joo HJ, Kong HJ, Kim HY. Tele-consent using mixed reality glasses (NREAL) in pediatric inguinal herniorrhaphy: a preliminary study. Scientific Reports. 2022 Feb 24;12(1):3105.

[27] Zhang X, Min G, Li T, Ma Z, Cao X, Wang S. AI and Blockchain Empowered Metaverse for Web 3.0: Vision, Architecture, and Future Directions. IEEE Communications Magazine. 2023 Jun 5.

