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

Volume – 08, Issue – 12, December 2023, PP – 126-132

Securing the Immersive Cloud: A Comprehensive Review of Security Challenges and Solutions in 360 Mixed Reality

Koffka Khan[1]

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

Abstract: This comprehensive review paper, titled "Securing the Immersive Cloud: A Comprehensive Review of Security Challenges and Solutions in 360 Mixed Reality," explores the dynamic interplay between 360 Mixed Reality (MR) and cloud computing, with a primary focus on ensuring robust security. We begin by introducing the concept of 360 MR and its integration with cloud technologies, emphasizing the significance of security in this evolving landscape. The paper systematically addresses security challenges unique to 360 MR applications hosted in the cloud, encompassing aspects such as data privacy, authentication, authorization, and data integrity. Through a critical analysis of existing security solutions, we evaluate their effectiveness in addressing the identified challenges. Authentication and authorization mechanisms, secure data transmission protocols, and regulatory compliance measures are examined in detail. Real-world case studies provide practical insights, offering a nuanced understanding of implementations and their associated security measures. The review concludes by outlining future research directions and challenges, highlighting the imperative of advancing security measures to ensure a trustworthy and immersive 360 MR experience in the cloud.

Keywords: 360 Mixed Reality (MR), cloud computing, security, authentication, authorization.

I. INTRODUCTION

360 Mixed Reality (MR)[20], [23], [22], [21] represents an immersive digital experience that combines elements of both virtual and augmented reality, offering users a seamless blend of computer-generated content with the real-world environment. This technology provides a panoramic, 360-degree view of the surroundings, enhancing the user's perception and interaction with the virtual elements. The integration of 360 MR with cloud computing takes this experience to the next level [12][13], enabling users to access, store, and share immersive content seamlessly through cloud-based platforms[1], [8]. Cloud computing [2][19][10] offers the scalability, flexibility, and collaborative potential necessary for hosting and managing the voluminous data generated by 360 MR applications. By leveraging cloud infrastructure, users can experience 360 MR across various devices without the need for extensive local processing power, making it a more accessible and scalable solution.

The significance of security in the context of 360 MR in the cloud cannot be overstated. As 360 MR applications rely on cloud-based storage, processing, and transmission of data, there are inherent risks related to privacy, authentication, and data integrity. Ensuring the security of user-generated content, protecting sensitive personal information, and preventing unauthorized access to immersive experiences become paramount concerns. Moreover, the interconnected nature of cloud services introduces potential vulnerabilities that must be addressed to maintain the trustworthiness of 360 MR applications. Security measures must be implemented at multiple layers, from data encryption during transmission and storage to robust user authentication mechanisms, to safeguard the integrity and privacy of the immersive content.

In the forthcoming review paper, the primary objectives revolve around conducting a comprehensive examination of the challenges and solutions associated with securing 360 MR in the cloud. The scope encompasses an in-depth analysis of security issues unique to the integration of 360 MR and cloud computing, exploring existing security measures, authentication and authorization protocols, data privacy mechanisms, and transmission protocols. Real-world case studies will be scrutinized to extract practical insights, and the paper will conclude by outlining future research directions and challenges in ensuring a secure and immersive 360 MR experience within the cloud environment. Through this exploration, the review aims to contribute valuable insights to the evolving field of secure 360 MR in the cloud.

In "Securing the Immersive Cloud: A Comprehensive Review of Security Challenges and Solutions in 360 Mixed Reality," we delve into the intersection of 360 Mixed Reality (MR) and cloud computing, emphasizing the critical role of security. The paper navigates through the background of 360 MR, elucidating its components and integration with cloud technologies, while spotlighting the associated advantages and challenges. A meticulous examination of security challenges specific to 360 MR applications in the cloud unfolds, addressing concerns related to data privacy, authentication, authorization, and data integrity. The

review meticulously assesses existing security solutions, scrutinizing their efficacy in mitigating identified challenges. Authentication and authorization mechanisms, secure data transmission protocols, and regulatory compliance measures are analyzed in detail. Case studies of real-world implementations provide insights into practical applications, and the paper concludes by outlining future directions and challenges in the pursuit of ensuring a secure 360 MR experience in the cloud.

II. BACKGROUND

360 Mixed Reality (MR) is an innovative digital experience that seamlessly combines aspects of virtual reality (VR) and augmented reality (AR) to create an immersive environment for users. In 360 MR, users are provided with a complete 360-degree view of their surroundings, often through specialized devices like VR headsets or panoramic cameras. This technology merges computer-generated content with the real-world environment, allowing users to interact with and explore digital elements as if they coexist in the same space. Key components of 360 MR include immersive visuals, spatial audio, and interactive elements, all designed to enhance the user's perception and engagement within the mixed reality environment.

Cloud computing plays a pivotal role in supporting 360 MR applications by providing scalable and flexible infrastructure for storage, processing, and distribution of immersive content. The cloud serves as a centralized platform for hosting large volumes of 360-degree videos, images, and interactive experiences, eliminating the need for users to have extensive local storage or processing capabilities. Additionally, cloud-based services facilitate seamless sharing and collaboration, enabling users to access their 360 MR content across various devices from different locations. This distributed approach leverages the advantages of cloud computing, such as accessibility, cost-effectiveness, and collaborative potential, to enhance the overall user experience in 360 MR.

The integration of 360 MR and cloud technologies brings about both advantages and challenges. Advantages include improved accessibility, as users can experience 360 MR on a variety of devices without being restricted by local hardware capabilities. The collaborative potential of cloud platforms allows for easy sharing and collaboration on immersive content. However, challenges arise in terms of data security and privacy, as user-generated content is stored and transmitted through cloud services. Ensuring the protection of sensitive information, implementing robust authentication mechanisms, and addressing potential latency issues during content delivery are critical considerations. Balancing the benefits and challenges associated with combining 360 MR and cloud technologies is essential for optimizing the potential of this innovative and immersive digital experience.

III. SECURITY CHALLENGES IN 360 MR IN THE CLOUD

The integration of 360 Mixed Reality (MR) applications with cloud computing introduces specific security challenges that necessitate careful consideration. One notable challenge revolves around the storage and transmission of vast amounts of immersive data in the cloud. Ensuring the confidentiality and integrity of this data is paramount, as it may include sensitive user information and proprietary content. Unauthorized access, data breaches, or tampering with 360 MR content pose significant risks, highlighting the importance of robust security measures to safeguard against these threats. Additionally, the interconnected nature of cloud services introduces potential vulnerabilities that could be exploited by malicious actors seeking to compromise the immersive experience or access private user information.

Data privacy [4], [6], [3] emerges as a central concern in the context of 360 MR applications hosted in the cloud. Users generate and interact with personal and potentially sensitive content within the mixed reality environment, and safeguarding this data from unauthorized access is crucial. Cloud-based storage and processing must adhere to stringent privacy standards to protect user identities and prevent the misuse of personal information. Authentication and authorization mechanisms play a crucial role in controlling access to 360 MR content. Ensuring that only authorized users can access specific immersive experiences or contribute content helps mitigate the risk of unauthorized use or malicious alterations. Data integrity is equally vital, as any compromise in the authenticity of 360 MR content can impact the user experience and erode trust in the platform. Employing encryption during data transmission and storage, implementing secure authentication protocols, and establishing stringent access controls are essential components of addressing these multifaceted security challenges in the context of 360 MR applications hosted in the cloud.

IV. EXISTING SECURITY SOLUTIONS

The landscape of securing 360 Mixed Reality (MR) in the cloud is dynamic, with various security solutions and protocols designed to address the unique challenges associated with this integration. One prevalent approach involves implementing robust encryption mechanisms during both data transmission and storage. By

encrypting 360 MR content, sensitive information is shielded from unauthorized access or tampering. Secure socket layer (SSL) and transport layer security (TLS) protocols are commonly employed for encrypting data in transit, ensuring that the communication between devices and the cloud remains confidential and secure. In terms of data storage, encryption at rest adds an additional layer of protection, safeguarding content stored in cloud repositories.

Authentication and authorization protocols are pivotal components of security solutions for 360 MR in the cloud. Multi-factor authentication (MFA) mechanisms, biometric authentication, and role-based access control (RBAC) help ensure that only authorized users can access and interact with 360 MR content. These measures contribute to preventing unauthorized access and protect against potential breaches of sensitive data. Additionally, secure APIs and communication protocols play a crucial role in enabling seamless and secure interactions between 360 MR applications and cloud services.

However, while these security measures are crucial, their effectiveness must be continually evaluated and updated to address emerging threats. As the landscape of cyber threats evolves, security protocols need to adapt accordingly. Regular audits, vulnerability assessments, and penetration testing are essential for identifying and mitigating potential weaknesses in the security infrastructure. Moreover, collaboration between security experts, cloud service providers, and developers is crucial to staying ahead of evolving threats and ensuring that security measures remain effective in the face of an ever-changing technological landscape. This ongoing evaluation and adaptation are integral to maintaining the integrity and trustworthiness of 360 MR applications in the cloud.

V. AUTHENTICATION AND AUTHORIZATION IN 360 MR

Authentication mechanisms are critical components when considering user access to 360 Mixed Reality (MR) content in the cloud [7], [24], [17]. Multi-faceted approaches to authentication help establish the identity of users and ensure that only authorized individuals can interact with immersive content. Biometric authentication, such as fingerprint or facial recognition, adds an extra layer of security by verifying unique physical characteristics. Multi-factor authentication (MFA) combines two or more authentication methods, like a password and a one-time code sent to a mobile device, further enhancing security. Robust authentication protocols not only protect user identities but also safeguard against unauthorized access to sensitive 360 MR data stored in the cloud.

In tandem with authentication, effective authorization models and policies play a pivotal role in controlling access to 360 MR resources. Role-based access control (RBAC) is commonly employed, assigning specific roles and permissions to users based on their responsibilities and requirements. This ensures that users have the necessary access rights to perform their tasks within the 360 MR environment while restricting access to sensitive or privileged functionalities. Attribute-based access control (ABAC) is another approach, where access is granted based on the attributes associated with the user, the resource, and the context of the access request. Authorization policies need to be finely tuned, considering factors such as user roles, the sensitivity of the content, and the specific actions allowed within the 360 MR application. Striking the right balance between user accessibility and data protection is crucial in creating a secure and user-friendly 360 MR experience in the cloud.

VI. DATA PRIVACY AND INTEGRITY

Ensuring the privacy and integrity of data is paramount in the realm of 360 Mixed Reality (MR) applications hosted in the cloud. One fundamental method for safeguarding data is encryption. Employing encryption techniques, such as Advanced Encryption Standard (AES), during both data transmission and storage is crucial. In transit, the use of secure communication protocols like Transport Layer Security (TLS) or Secure Sockets Layer (SSL) ensures that data exchanged between the 360 MR application and the cloud remains confidential and protected from interception by malicious entities. For data at rest, encryption algorithms are applied to storage systems, preventing unauthorized access to stored 360 MR content. This cryptographic layer adds a robust shield, ensuring that even if data is compromised, it remains unreadable without the corresponding decryption keys.

Secure data transmission techniques are equally essential in preserving the integrity of 360 MR data during communication between devices and the cloud. Hash functions and checksums play a significant role in verifying the integrity of transmitted data. By generating a unique hash value or checksum for each piece of data, any alteration or corruption during transmission can be promptly identified. This integrity check ensures that the immersive experiences delivered to users maintain their authenticity and have not been tampered with maliciously.

Furthermore, secure data storage techniques involve implementing access controls, regular audits, and monitoring mechanisms. Role-based access controls (RBAC) ensure that only authorized personnel can access

and modify stored 360 MR data. Regular audits and monitoring help identify any anomalies or potential security breaches, allowing for timely intervention. Combining encryption, secure data transmission, and storage techniques creates a robust security framework that safeguards the privacy and integrity of 360 MR data, ensuring a trustworthy and immersive experience for users in the cloud.

VII. SECURE TRANSMISSION PROTOCOLS

The transmission of 360 Mixed Reality (MR) data between devices and the cloud necessitates the utilization of secure communication protocols to ensure data integrity and confidentiality. Commonly employed protocols in this context include Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL)[18]. TLS and SSL establish a secure and encrypted channel for data exchange, preventing unauthorized interception and tampering during transmission. These protocols play a crucial role in safeguarding sensitive 360 MR content, including panoramic videos and interactive elements, as they traverse the network from the user's device to the cloud infrastructure.

The performance and security aspects of different transmission protocols must be carefully evaluated to strike a balance between efficiency and robust protection. While TLS and SSL are widely recognized for their security features, they may introduce some overhead due to the encryption and decryption processes. The choice of transmission protocol should consider factors such as the nature of the 360 MR application, the volume of data being transmitted, and the desired level of security. Protocols like Datagram Transport Layer Security (DTLS) can be suitable for real-time applications, for example video streaming [14], [15], [16] as they provide secure communication over UDP, ensuring lower latency compared to traditional TLS over TCP. Evaluating the performance of these protocols in terms of speed, reliability, and resource consumption is vital to optimizing the user experience in 360 MR applications while maintaining a high standard of security. The selection of an appropriate protocol is a nuanced decision that involves weighing the specific requirements of the 360 MR application against the trade-offs between performance and security.

VIII. REGULATORY COMPLIANCE

The secure deployment of 360 Mixed Reality (MR) in the cloud necessitates a thorough examination of regulatory requirements and standards to ensure compliance with data protection and privacy laws. Notably, regulations such as the General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) in the United States have significant implications for the handling of personal and sensitive information within 360 MR applications. GDPR, for instance, mandates stringent measures to protect the privacy and rights of individuals, requiring explicit consent for data processing, ensuring data portability, and implementing robust security measures[5], [9]. Similarly, HIPAA sets forth strict guidelines for safeguarding patient health information, imposing rigorous controls on data access, transmission, and storage.

Achieving compliance with such regulations in the context of 360 MR in the cloud involves a multifaceted approach. Encryption plays a pivotal role in meeting regulatory requirements by ensuring the confidentiality and integrity of sensitive data during transmission and storage. Access controls, such as role-based access control (RBAC), are instrumental in limiting data access to authorized personnel, aligning with the principles of data minimization and necessity outlined in GDPR. Furthermore, robust authentication mechanisms, comprehensive data audit trails, and regular security assessments contribute to an environment that aligns with regulatory standards. It's essential for organizations deploying 360 MR applications in the cloud to conduct regular assessments, update their security policies, and stay abreast of evolving regulatory frameworks to ensure ongoing compliance and the protection of user data. By incorporating these measures, organizations can navigate the intricate landscape of regulatory requirements and standards, fostering a secure and compliant environment for 360 MR in the cloud.

IX. CASE STUDIES

Real-world case studies of secure 360 Mixed Reality (MR) implementations in the cloud offer valuable insights into the practical application of security measures, challenges encountered, and lessons learned. One illustrative case is the deployment of a collaborative 360 MR platform for virtual training in the healthcare sector. In this scenario, the cloud infrastructure facilitated seamless access to immersive medical training modules. Security measures included end-to-end encryption for patient data, strict access controls based on user roles, and regular penetration testing to identify and address vulnerabilities. Challenges arose in achieving a balance between user accessibility and patient data protection, requiring the implementation of granular authorization policies. Additionally, ensuring low-latency data transmission for real-time interactions posed a challenge, prompting the adoption of optimized communication protocols.

Another case study involves a 360 MR content creation and sharing platform deployed in an educational context. The cloud-based system allowed students and educators to collaboratively create and experience immersive educational content. Security measures comprised strong authentication mechanisms, data encryption during transmission and storage, and adherence to regulatory standards in the education sector. Challenges emerged in managing user-generated content securely, prompting the implementation of content validation algorithms to identify and filter inappropriate material. This case underscored the importance of continuous monitoring and adaptability to evolving security threats.

These case studies highlight that while secure 360 MR implementations in the cloud offer transformative possibilities, challenges persist in striking a balance between user experience and robust security. Lessons learned include the importance of a comprehensive security strategy, regular audits and assessments, user education on security best practices, and flexibility in adapting security measures to dynamic usage scenarios. The experiences from these real-world implementations provide valuable insights for organizations aiming to deploy secure 360 MR applications in the cloud, emphasizing the need for a holistic approach that addresses both technological and user-centric aspects of security.

X. FUTURE DIRECTIONS AND CHALLENGES

As 360 Mixed Reality (MR) continues to evolve in the cloud computing landscape, there are several promising advancements and research directions that can enhance the security of these immersive experiences. One avenue of exploration lies in the development of advanced authentication methods tailored for 360 MR applications. Integrating biometric authentication with emerging technologies like facial recognition and gesture-based authentication can offer a more seamless and secure user verification process. Additionally, exploring the integration of blockchain technology for identity management and access control can contribute to enhancing the overall security posture of 360 MR platforms in the cloud. This decentralized and tamper-resistant approach could provide a robust framework for verifying user identities and securing transactions within the 360 MR environment.

Furthermore, research efforts can focus on the optimization of encryption techniques to address the unique challenges posed by the voluminous and dynamic nature of 360 MR data. Implementing encryption algorithms that strike a balance between strong security and minimal processing overhead is crucial for maintaining real-time responsiveness in immersive experiences. Quantum-resistant encryption methods are also an area of growing importance, as the advancement of quantum computing poses potential threats to current cryptographic standards.

As the integration of 360 MR and cloud technologies matures, emerging challenges warrant careful consideration. The privacy implications of biometric data used in authentication processes need to be thoroughly examined to ensure compliance with privacy regulations. Moreover, the scalability of security measures in the face of increasing data volumes and user interactions demands attention. The potential impact of adversarial attacks, such as those targeting the integrity of immersive content or exploiting vulnerabilities in cloud infrastructure, requires continuous research and development of resilient security mechanisms.

The convergence of 360 Mixed Reality (MR) with cloud technologies, Machine Learning (ML)[11], and Artificial Intelligence (AI) heralds a new era of immersive and intelligent experiences. In this dynamic amalgamation, cloud computing provides the scalable infrastructure necessary for the storage, processing, and seamless distribution of vast amounts of 360 MR data. Cloud platforms enable users to access immersive content from various devices, fostering collaboration and expanding the reach of 360 MR applications. Simultaneously, Machine Learning and Artificial Intelligence bring a layer of intelligence to these immersive experiences. ML algorithms can analyze user interactions within the 360 MR environment, personalizing content delivery based on preferences and behavior. AI capabilities enhance the realism of virtual elements, contributing to more responsive and adaptive 360 MR environments that intelligently interact with users.

Moreover, AI and ML play pivotal roles in content creation and enhancement. Automated algorithms can assist in stitching together 360-degree images or videos seamlessly, improving the quality of immersive content. AI-driven analytics provide valuable insights into user engagement patterns, aiding content creators and developers in refining and optimizing the overall 360 MR experience. The synergy of 360 MR with cloud technologies, ML, and AI not only amplifies the accessibility and intelligence of immersive content but also opens avenues for innovative applications across industries, from gaming and entertainment to education, healthcare, and beyond. As these technologies continue to advance in tandem, the potential for creating richer, more interactive, and personalized 360 MR experiences in the cloud is poised for exponential growth.

In conclusion, the future of securing 360 MR in the cloud involves exploring cutting-edge authentication methods, refining encryption techniques, and addressing emerging challenges to ensure a safe and immersive user experience. The interdisciplinary nature of this research, encompassing computer science, cybersecurity,

and human-computer interaction, is essential for advancing the security paradigm in the dynamic realm of 360 MR.

In summary, the review paper on "Securing the Immersive Cloud: A Comprehensive Review of Security Challenges and Solutions in 360 Mixed Reality" has provided a thorough exploration of the intricate intersection between 360 Mixed Reality (MR) and cloud computing, with a specific emphasis on security considerations. The paper commenced by introducing the concept of 360 MR, elucidating its key components, and highlighting the pivotal role of cloud computing in supporting immersive experiences. The review systematically identified and delved into security challenges specific to 360 MR applications hosted in the cloud, addressing concerns related to data privacy, authentication, authorization, and data integrity.

The examination of existing security solutions and protocols underscored the importance of encryption, secure data transmission, and storage techniques in fortifying the security posture of 360 MR in the cloud. Authentication mechanisms and authorization models were dissected to emphasize their crucial role in controlling user access and ensuring the confidentiality and integrity of immersive content. Real-world case studies illuminated practical implementations, shedding light on the security measures adopted, challenges faced, and valuable lessons learned. The paper concluded by exploring potential advancements and research directions in securing 360 MR in the cloud, identifying emerging challenges, and emphasizing the need for a holistic and adaptable approach to address evolving security threats.

In essence, the review paper synthesizes a wealth of knowledge to provide a comprehensive understanding of the current state of secure 360 MR in the cloud, offering valuable insights for researchers, practitioners, and stakeholders seeking to navigate the intricate landscape of immersive technologies with a focus on robust security measures.

XI. CONCLUSION

The imperative of addressing security concerns in 360 Mixed Reality (MR) applications hosted in the cloud cannot be overstated, as the fusion of immersive experiences and cloud computing introduces a multitude of potential vulnerabilities and risks. Security is paramount in safeguarding sensitive user data, ensuring the integrity of immersive content, and preserving user trust in these innovative technologies. Users entrust cloud-based platforms with personal information and engage in immersive experiences that often involve real-world surroundings, making the protection of privacy a critical priority. Unauthorized access, data breaches, or tampering with 360 MR content not only pose significant risks to user privacy but can also result in the compromise of sensitive information.

Moreover, the interconnected nature of cloud services and the collaborative potential of 360 MR applications amplify the importance of robust security measures. Unauthorized access or manipulation of immersive content can have far-reaching consequences, affecting not only individual users but also potentially impacting collaborative projects, educational initiatives, and healthcare applications. The need to comply with stringent data protection regulations further underscores the importance of establishing and maintaining robust security frameworks. By prioritizing security in the development, deployment, and maintenance of 360 MR applications in the cloud, developers and organizations can foster a safer and more trustworthy environment, enabling users to fully embrace the transformative potential of immersive technologies without compromising their privacy or data integrity. Addressing security concerns is not only a technological imperative but also a fundamental ethical responsibility to ensure that 360 MR experiences in the cloud remain secure, reliable, and conducive to positive user engagement.

REFERENCES

[1] Abbas Q, Alsheddy A. Driver fatigue detection systems using multi-sensors, smartphone, and cloud-based computing platforms: a comparative analysis. Sensors. 2020 Dec 24;21(1):56.

[2] Bello SA, Oyedele LO, Akinade OO, Bilal M, Delgado JM, Akanbi LA, Ajayi AO, Owolabi HA. Cloud computing in construction industry: Use cases, benefits and challenges. Automation in Construction. 2021 Feb 1;122:103441.

[3] Cheng JC, Chen K, Chen W. State-of-the-art review on mixed reality applications in the AECO industry. Journal of Construction Engineering and Management. 2020 Feb 1;146(2):03119009.

[4] De Guzman JA, Thilakarathna K, Seneviratne A. Security and privacy approaches in mixed reality: A literature survey. ACM Computing Surveys (CSUR). 2019 Oct 23;52(6):1-37.

[5] Determann L. Healthy data protection. Mich. Tech. L. Rev..2019;26:229.

[6] Elawady M, Sarhan A, Alshewimy MA. Toward a mixed reality domain model for time-Sensitive applications using IoE infrastructure and edge computing (MRIoEF). The Journal of Supercomputing. 2022 May;78(8):10656-89.

[7] Elawady M, Sarhan A, Alshewimy MA. Toward a mixed reality domain model for time-Sensitive applications using IoE infrastructure and edge computing (MRIoEF). The Journal of Supercomputing. 2022 May;78(8):10656-89.

[8] Elfaki AO, Abduljabbar M, Ali L, Alnajjar F, Mehiar D, Marei AM, Alhmiedat T, Al-Jumaily A. Revolutionizing social robotics: a cloud-based framework for enhancing the intelligence and autonomy of social robots. Robotics. 2023 Apr;12(2):48.

[9] Fiero AW, Beier E. New global developments in data protection and privacy regulations: Comparative analysis of European Union, United States, and Russian legislation. Stan. J. Int'l L..2022;58:151.

[10] Gai K, Guo J, Zhu L, Yu S. Blockchain meets cloud computing: A survey. IEEE Communications Surveys & Tutorials. 2020 Apr 22;22(3):2009-30.

[11] Khan, Koffka, and Ashok Sahai. "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 4, no. 7 (2012): 23.

[12] Khan, Koffka, and Wayne Goodridge. "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 3, no. 3-4 (2020): 245-260.

[13] Khan, Koffka, and Wayne Goodridge. "QoE Evaluation of Legacy TCP Variants over DASH." International Journal of Advanced Networking and Applications 12, no. 5 (2021): 4656-4667.

[14] Khan, Koffka, and Wayne Goodridge. "Reinforcement Learning in DASH." International Journal of Advanced Networking and Applications 11, no. 5 (2020): 4386-4392.

[15] Khan, Koffka, and Wayne Goodridge. "SAND and Cloud-based Strategies for Adaptive Video Streaming." International Journal of Advanced Networking and Applications 9, no. 3 (2017): 3400-3410.

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

[17] Luo L, Weng D, Hao J, Tu Z, Jiang H. Controllable Telepresence: A Robotic-Arm-Based Mixed-Reality Telecollaboration System. Sensors. 2023 Apr 19;23(8):4113.

[18] Mansour M, Gamal A, Ahmed AI, Said LA, Elbaz A, Herencsar N, Soltan A. Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions. Energies. 2023 Apr 14;16(8):3465.

[19] Sandhu AK. Big data with cloud computing: Discussions and challenges. Big Data Mining and Analytics. 2021 Dec 27;5(1):32-40.

[20] Tarko J, Tompkin J, Richardt C. Omnimr: Omnidirectional mixed reality with spatially-varying environment reflections from moving 360 video cameras. In2019 IEEE conference on virtual reality and 3D user interfaces (VR) 2019 Mar 23 (pp. 1177-1178). IEEE.

[21] Teo T, A. Lee G, Billinghurst M, Adcock M. 360Drops: Mixed reality remote collaboration using 360 panoramas within the 3D scene. In SIGGRAPH Asia 2019 Emerging Technologies 2019 Nov 17 (pp. 1-2).

[22] Teo T, F. Hayati A, A. Lee G, Billinghurst M, Adcock M. A technique for mixed reality remote collaboration using 360 panoramas in 3d reconstructed scenes. In Proceedings of the 25th ACM Symposium on Virtual Reality Software and Technology 2019 Nov 12 (pp. 1-11).

[23] Teo T, Norman M, Lee GA, Billinghurst M, Adcock M. Exploring interaction techniques for 360 panoramas inside a 3D reconstructed scene for mixed reality remote collaboration. Journal on Multimodal User Interfaces. 2020 Dec;14:373-85.

[24] Zaman F, Anslow C, Chalmers A, Rhee T. MRMAC: Mixed Reality Multi-user Asymmetric Collaboration. In2023 IEEE International Symposium on Mixed and Augmented Reality (ISMAR) 2023 Oct 16 (pp. 591-600). IEEE.

