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

Volume – 08, Issue – 12, December 2023, PP – 85-91

# Securing the Augmented Horizon: A Comprehensive Review of Secure 360 Augmented Reality in Cloud Environments

Koffka Khan[1]

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

**Abstract:** "Securing the Augmented Horizon: A Comprehensive Review of Secure 360 Augmented Reality in Cloud Environments" explores the intersection of augmented reality (AR) and cloud computing, delving into the imperative need for robust security measures within this dynamic landscape. Beginning with an overview of AR's evolution and integration with cloud technologies, the paper addresses the security challenges inherent in AR applications hosted on the cloud. It defines and examines the concept of Secure 360 Augmented Reality, emphasizing the significance of a holistic security approach. The integration of AR and cloud computing is discussed, with a focus on the advantages, challenges, and the role of cloud services in enhancing accessibility and scalability. The paper scrutinizes common security challenges, including data privacy, authentication, and data integrity, while proposing comprehensive security measures, such as encryption and secure communication protocols. Case studies highlight real-world implementations, offering insights into successful security practices. The paper concludes by identifying current challenges, outlining potential future developments, and emphasizing the pivotal role of security in shaping the future of AR in cloud environments.

**Keywords:** 360 Augmented Reality, Cloud Environments, security, data privacy, authentication, integrity.

## I. INTRODUCTION

The fusion of 360-degree augmented reality (AR) [16], [20], [3] with cloud computing [17], [13], [1] represents a paradigm shift in immersive digital experiences. 360 AR extends the immersive capabilities of traditional augmented reality by providing a panoramic view of the surrounding environment. This innovation allows users to interact seamlessly with digitally enhanced elements superimposed onto their real-world surroundings, fostering a more immersive and engaging user experience [5], [6]. Applications of 360 AR span a multitude of domains, including gaming, video streaming [7], [8], [10], education, healthcare, and industrial training. The panoramic augmentation enhances spatial awareness, creating a more natural and intuitive interaction with digital content.

As the demand for richer and more complex mixed reality experiences intensifies, the role of cloud computing becomes increasingly pivotal. Cloud infrastructure offers scalable and flexible resources, allowing for the storage, processing, and distribution of the vast amounts of data inherent in 360 AR applications. Leveraging the cloud facilitates real-time rendering, content delivery, and collaboration, overcoming the limitations of local processing power. This symbiotic relationship between 360 AR and cloud computing not only enhances the user experience but also enables cross-platform accessibility, making augmented reality applications more accessible and versatile.

However, as 360 AR applications migrate to the cloud, the paramount importance of ensuring robust security measures cannot be overstated. The integration of personal, sensitive, or proprietary information within these immersive experiences necessitates stringent safeguards to protect against potential cyber threats. From data privacy concerns to authentication and authorization challenges, the security landscape for 360 AR in the cloud is multifaceted. Addressing these issues is crucial to foster user trust, safeguard intellectual property, and ensure the seamless deployment and adoption of 360 AR applications in cloud environments.

"Securing the Augmented Horizon: A Comprehensive Review of Secure 360 Augmented Reality in Cloud Environments" explores the intersection of augmented reality (AR) and cloud computing, delving into the imperative need for robust security measures within this dynamic landscape. Beginning with an overview of AR's evolution and integration with cloud technologies, the paper addresses the security challenges inherent in AR applications hosted on the cloud. It defines and examines the concept of Secure 360 Augmented Reality, emphasizing the significance of a holistic security approach. The integration of AR and cloud computing is discussed, with a focus on the advantages, challenges, and the role of cloud services in enhancing accessibility and scalability. The paper scrutinizes common security challenges, including data privacy, authentication, and data integrity, while proposing comprehensive security measures, such as encryption and secure communication protocols. Case studies highlight real-world implementations, offering insights into successful security practices.

  

The paper concludes by identifying current challenges, outlining potential future developments, and emphasizing the pivotal role of security in shaping the future of AR in cloud environments.

## II. BACKGROUND

The evolution of 360-degree augmented reality (AR) technologies has been marked by a transformative journey from traditional AR applications to immersive experiences that envelop users in a 360-degree digital environment. Initially, AR primarily involved overlaying digital information onto the real world through devices like smartphones and tablets. The advent of 360-degree AR introduced a more comprehensive spatial understanding by capturing and integrating the entire surroundings into the augmented experience. This shift allows users to explore and interact with a fully immersive digital layer seamlessly integrated with their physical environment. The technologies involved include advanced sensors, cameras, and processing capabilities to create a panoramic view that responds dynamically to user movements. The evolution of 360 AR has expanded its applications across diverse sectors, from entertainment and education to industrial training and healthcare.

The integration of mixed reality, including 360 AR, with cloud computing represents a strategic synergy that enhances the scalability and efficiency of these immersive experiences. Cloud computing provides a robust infrastructure for hosting, processing, and distributing the vast amounts of data generated by 360 AR applications. The cloud's scalability allows for real-time rendering and collaboration, overcoming the limitations of local processing power. This integration fosters a more seamless and responsive user experience, enabling developers to create richer and more interactive 360 AR content. Additionally, cloud-based deployment facilitates cross-platform accessibility, making augmented reality experiences more versatile and readily available to a wider audience.

Despite the numerous advantages of integrating mixed reality with cloud computing, this convergence introduces a set of security challenges. The immersive nature of 360 AR experiences often involves the collection and processing of sensitive data, such as user location or real-time interactions. Security concerns include protecting this data from unauthorized access, ensuring the integrity of the augmented content, and safeguarding against potential cyber threats. Authentication and authorization mechanisms become critical in mixed reality and cloud environments to manage user access and prevent unauthorized manipulation of digital overlays. Addressing these security challenges is imperative to establish trust among users, organizations, and developers and to foster the widespread adoption of 360 AR in cloud-based applications.

## III. RELATED WORK

The existing literature on 360 Augmented Reality (AR) security and cloud security reveals a growing body of research dedicated to addressing the unique challenges posed by the integration of immersive technologies with cloud computing. Studies often delve into the intersection of data privacy, user authentication, and the protection of sensitive information within the context of 360 AR applications hosted on cloud platforms. Researchers have examined the evolution of security protocols and frameworks, seeking to adapt traditional security measures to the dynamic and interactive nature of mixed reality environments.

Key studies in this domain explore methodologies for securing 360 AR experiences in the cloud. These methodologies often involve a combination of encryption techniques, access controls, and secure data transmission protocols to protect against unauthorized access and data breaches. Additionally, researchers have investigated the role of secure cloud architectures in mitigating potential risks associated with the storage and processing of large volumes of data inherent in 360 AR applications. The findings underscore the importance of implementing robust security measures at various layers, from the device capturing the real-world environment to the cloud infrastructure managing and delivering the augmented content.

The overarching goal of these studies is to provide insights into best practices for securing 360 AR in the cloud, ensuring the confidentiality, integrity, and availability of data and interactions. By identifying potential vulnerabilities and proposing effective security strategies, the literature contributes to the development of a secure foundation for the widespread adoption of 360 AR applications in cloud environments. This ongoing research underscores the interdisciplinary nature of the field, involving expertise in computer science, information security, and human-computer interaction to create a holistic understanding of the challenges and solutions at the intersection of 360 AR and cloud security.

## IV. 360 MIXED REALITY IN CLOUD ARCHITECTURE

The architecture of 360 Augmented Reality (AR) systems deployed in the cloud is a sophisticated integration of hardware components and cloud-based services, designed to deliver immersive and responsive experiences to users. At its core, the architecture is characterized by a decentralized and distributed model, with various components working in tandem to capture, process, store, and present augmented content seamlessly.

  

Capture devices, such as 360-degree cameras or sensors, play a pivotal role in capturing the user's real-world environment. These devices are equipped to capture a panoramic view, enabling a comprehensive understanding of the physical space.

Once the real-world environment is captured, the data is transmitted to the cloud for processing. Cloud-based processing units are responsible for handling the computational demands of rendering and augmenting the captured environment in real-time. These processing units leverage the scalability and parallel processing capabilities of cloud infrastructure to ensure smooth and responsive interactions. The processed data, including augmented overlays and spatial information, is then stored in cloud-based storage solutions. This storage serves as a repository for the vast amounts of data generated by 360 AR applications, enabling efficient retrieval and access.

User interfaces in 360 AR systems[12], [9], [14] act as the bridge between the augmented content and the end-user. These interfaces can take various forms, including headsets, smartphones, or AR glasses, providing users with the means to visualize and interact with the augmented environment. The cloud-based architecture ensures that the user interface devices can access and retrieve augmented content seamlessly from the cloud, facilitating a dynamic and responsive user experience. In summary, the architecture of 360 AR systems in the cloud is a complex and interconnected network of capture, processing, storage, and user interface components, leveraging cloud computing's scalability and distributed nature to deliver immersive and interactive augmented reality experiences.

## V. SECURITY CHALLENGES

The integration of 360 Augmented Reality (AR) with cloud computing introduces a set of security challenges [19], [15], [21], [11] that necessitate careful consideration to ensure the integrity, confidentiality, and availability of sensitive data. One prominent challenge lies in the realm of data privacy, as 360 AR applications often involve the capture and processing of user-generated content and real-world environments. The potential exposure of personal or proprietary information demands robust measures to safeguard against unauthorized access and mitigate the risk of privacy breaches. Cloud-based storage and transmission of this data pose additional challenges, requiring encryption and secure protocols to protect against interception and unauthorized retrieval.

Maintaining the integrity of augmented content is another critical concern in the 360 AR and cloud environment. With the distributed nature of cloud computing, ensuring that augmented overlays remain unaltered during storage, processing, and transmission is paramount. Authentication becomes a crucial aspect, as verifying the identity of users and devices interacting with the augmented content helps prevent malicious manipulation or unauthorized modifications. Strong authentication mechanisms, such as multi-factor authentication, are essential to mitigate the risk of unauthorized access to both the captured real-world data and the augmented digital overlays.

Authorization mechanisms are integral to controlling and regulating access to 360 AR content in the cloud. Determining who has permission to view, modify, or share augmented content is essential for preventing unauthorized use and potential misuse of sensitive information. Effective authorization strategies involve defining roles, access levels, and permissions, and are crucial in maintaining a secure environment for 360 AR applications. In summary, the security challenges specific to 360 AR in a cloud environment encompass data privacy concerns, the preservation of data integrity, robust authentication measures, and well-defined authorization mechanisms, all of which are fundamental to building a secure foundation for the deployment of immersive augmented reality experiences in the cloud.

## VI. SECURITY SOLUTIONS AND TECHNOLOGIES

As the demand for secure 360 Augmented Reality (AR) experiences in the cloud continues to grow, both existing and emerging security solutions are playing a crucial role in mitigating potential risks and safeguarding sensitive data. Encryption techniques form a cornerstone of these security measures, ensuring the confidentiality of data during transmission and storage. End-to-end encryption protocols are often employed to protect the data as it travels between capture devices, cloud servers, and user interface devices. This cryptographic approach prevents unauthorized access and eavesdropping, maintaining the privacy of both the real-world environment captured by 360 AR and the augmented overlays generated in the cloud.

Access controls in the context of 360 AR in the cloud involve defining and managing permissions to access, modify, or interact with augmented content. Role-based access control (RBAC) systems are commonly implemented, assigning specific roles and privileges to users based on their responsibilities and requirements. This ensures that only authorized individuals can manipulate or view sensitive augmented content, reducing the risk of unauthorized modifications or data breaches. Furthermore, access controls extend to managing

  

permissions at different levels within the cloud infrastructure, including storage, processing, and transmission layers, to create a comprehensive security framework.

Authentication methods tailored for mixed reality applications in the cloud address the need to verify the identity of users and devices interacting with augmented content. Multi-factor authentication (MFA), biometric authentication, and device authentication are among the techniques employed to enhance security. MFA, for instance, requires users to provide multiple forms of identification, such as a password and a unique code sent to their mobile device, adding an extra layer of security against unauthorized access. The integration of these authentication methods ensures that only authenticated and authorized entities can engage with the immersive 360 AR experiences, contributing to a robust and secure deployment in the cloud. In essence, the combination of encryption techniques, access controls, and authentication methods forms a comprehensive security framework tailored to the unique challenges and requirements of 360 AR in the cloud.

## VII. CASE STUDIES

Several real-world examples and case studies showcase the successful implementation of secure 360 Augmented Reality (AR) in the cloud, highlighting the effective security measures deployed to ensure the integrity and confidentiality of augmented content. One notable case is the deployment of 360 AR in enterprise training scenarios. Companies have embraced the immersive capabilities of 360 AR to provide employees with realistic and interactive training experiences. These applications often involve cloud-based platforms that facilitate content storage, processing, and seamless delivery to various training locations. Security measures in such cases include end-to-end encryption for transmitted data, robust access controls to restrict content access to authorized personnel, and secure authentication methods to verify the identity of trainees participating in the augmented training modules.

In the realm of healthcare, secure 360 AR applications have been utilized for medical training, surgical simulations, and patient education. Cloud-based platforms enable the storage and retrieval of detailed 360 AR medical models, ensuring accessibility to healthcare professionals regardless of their physical location. Security measures in these healthcare applications encompass strict access controls to protect patient data, encryption of sensitive medical imagery, and secure authentication to guarantee that only qualified healthcare professionals can interact with and interpret the augmented medical content.

Moreover, entertainment and marketing industries have leveraged secure 360 AR in cloud environments to create immersive and engaging experiences. Virtual tours, interactive product demonstrations, and marketing campaigns have incorporated 360 AR technology, often relying on cloud infrastructure for content storage and delivery. Security measures implemented in these cases include encryption of promotional and proprietary content, robust access controls to protect intellectual property, and secure authentication methods to verify the credentials of individuals creating or managing the augmented marketing materials.

Across these diverse examples, a common thread is the integration of encryption, access controls, and authentication mechanisms tailored to the specific needs of each application. These security measures collectively contribute to the successful implementation of 360 AR in the cloud, fostering user trust, protecting sensitive data, and promoting the widespread adoption of secure and immersive augmented reality experiences across various industries.

## VIII. FUTURE TRENDS AND CHALLENGES

The future of 360 Augmented Reality (AR) in the context of cloud computing holds exciting possibilities and transformative trends. One emerging trend is the integration of artificial intelligence (AI) and machine learning (ML)[4] algorithms to enhance the interactive and adaptive nature of 360 AR experiences. Advanced algorithms can analyze user behaviors, preferences, and environmental data in real-time, enabling more personalized and context-aware augmented content. Cloud platforms will play a pivotal role in supporting the computational demands of these AI-driven enhancements, allowing for dynamic content generation and adaptation based on user interactions and the evolving real-world environment.

Another future trend is the proliferation of extended reality (XR) ecosystems, which combine augmented reality, virtual reality, and mixed reality technologies. Cloud computing will serve as the backbone for these interconnected ecosystems, facilitating seamless transitions between different reality modalities. This integration will lead to more immersive and versatile experiences, allowing users to seamlessly move between augmented and virtual environments while leveraging the computational power and storage capabilities of the cloud.

However, with these promising trends come anticipated challenges in securing evolving mixed reality technologies. One significant challenge is the potential escalation of cyber threats and attacks targeting the interconnected nature of 360 AR and cloud ecosystems. As mixed reality applications become more sophisticated, the attack surface widens, necessitating robust cybersecurity measures. Solutions may include the

  

implementation of advanced threat detection systems, continuous monitoring, and the development of adaptive security protocols that can dynamically respond to emerging threats.

Additionally, privacy concerns are expected to become more pronounced as 360 AR applications increasingly involve the capture and processing of detailed real-world environments. Striking a balance between delivering immersive experiences and safeguarding user privacy will require the development of privacy-preserving technologies, such as anonymization techniques and decentralized data processing approaches. Ensuring transparent data practices and obtaining user consent will be essential components of addressing privacy challenges.

In conclusion, the future trends in 360 AR and cloud computing promise groundbreaking advancements in user experiences and interconnected reality ecosystems. However, addressing challenges related to cybersecurity and privacy will be imperative to foster user trust and the responsible development of secure and ethically sound mixed reality technologies. The continued collaboration between technologists, policymakers, and industry stakeholders will play a pivotal role in shaping the trajectory of 360 AR in the cloud.

## IX. BEST PRACTICES FOR SECURE DEPLOYMENT

Deploying 360 Augmented Reality (AR) securely in the cloud requires organizations to adhere to rigorous guidelines and best practices to ensure the confidentiality, integrity, and availability of sensitive data. One fundamental aspect is to conduct a comprehensive risk assessment before implementation. This involves identifying potential threats, vulnerabilities, and risks associated with the deployment of 360 AR in the cloud. By understanding the unique security challenges and potential points of weakness, organizations can develop a targeted security strategy tailored to their specific use cases and requirements.

Establishing robust access controls is a key best practice to enforce secure deployment. Organizations should implement role-based access control (RBAC) mechanisms[2][18], defining roles and permissions for individuals based on their responsibilities. This helps restrict access to sensitive augmented content, ensuring that only authorized personnel can view, modify, or manage the data. Additionally, implementing strong authentication measures, such as multi-factor authentication, adds an extra layer of protection against unauthorized access.

Strategies for risk management and compliance involve adopting a proactive approach to security. Organizations should continuously monitor and assess the evolving threat landscape, staying informed about the latest security vulnerabilities and updates. Regular audits and penetration testing can help identify potential weaknesses in the deployment, enabling organizations to address vulnerabilities before they can be exploited. Compliance with industry regulations and standards, such as GDPR or HIPAA, is critical for organizations handling sensitive data. Implementing encryption protocols, secure data transmission practices, and ensuring data residency compliance are essential elements of a robust risk management and compliance strategy.

Moreover, organizations should prioritize user education and awareness. Providing training on secure usage practices for both employees and end-users can significantly mitigate risks associated with unintentional security breaches. Regularly updating and patching software, including both the 360 AR application and the underlying cloud infrastructure, is vital to address known vulnerabilities and enhance the overall security posture.

In summary, secure deployment of 360 AR in the cloud requires a multifaceted approach encompassing risk assessment, access controls, authentication mechanisms, compliance adherence, and continuous monitoring. By incorporating these guidelines and best practices, organizations can create a resilient and secure environment for leveraging the transformative capabilities of 360 Augmented Reality in the cloud.

In summary, the review of 360 Augmented Reality (AR) in the cloud underscores the transformative potential of immersive technologies and their integration with cloud computing. Key findings highlight the evolution of 360 AR technologies, the complex architecture of cloud-based systems, security challenges specific to this domain, existing and emerging security solutions, real-world applications, and future trends. The examination of case studies reveals successful implementations in various sectors, showcasing the versatility and promise of 360 AR in enhancing training, healthcare, marketing, and entertainment experiences.

Emphasizing the importance of addressing security concerns in 360 AR deployments in the cloud is paramount to ensuring the sustained growth and adoption of these innovative technologies. As organizations increasingly leverage the immersive capabilities of 360 AR in cloud environments, they must recognize and prioritize security as a foundational element of their deployment strategies. The unique challenges, such as data privacy, integrity, and authentication, necessitate robust security measures tailored to the dynamic and interconnected nature of mixed reality experiences. The integration of encryption techniques, access controls, and authentication methods, as well as the proactive management of risks and compliance, becomes crucial for fostering user trust, protecting sensitive data, and mitigating potential cyber threats.

  

Security concerns in 360 AR are not merely technical challenges but also encompass ethical considerations related to user privacy and responsible data handling. As these technologies become more prevalent in our daily lives, it is imperative for organizations to adopt a holistic approach that combines technological safeguards with transparent practices and user education. By prioritizing security at every stage of the deployment lifecycle, from design and development to implementation and maintenance, organizations can ensure the integrity and success of 360 AR experiences in the cloud, thereby contributing to a secure and ethically sound future for immersive technologies.

## X. CONCLUSION

In contemplating the future of 360 Augmented Reality (AR) in the cloud, several promising avenues for future research emerge. One compelling area of exploration involves the enhancement of user interactions through the integration of artificial intelligence (AI) and machine learning (ML) algorithms. Researchers can delve into developing intelligent algorithms that analyze user behaviors, preferences, and contextual data in real-time. This approach aims to dynamically adapt and personalize augmented content, creating more immersive and user-centric experiences. Investigating how AI-driven algorithms can optimize content generation, enhance spatial understanding, and respond intelligently to user input would contribute significantly to the advancement of 360 AR applications in the cloud.

Another prospective area for research revolves around addressing the ethical implications and societal impacts of 360 AR technologies. As these immersive experiences become more prevalent, researchers can explore the ethical considerations related to data privacy, consent, and the potential influence of augmented content on user perceptions and behaviors. Investigating frameworks for responsible development and deployment of 360 AR applications in cloud environments will be essential. This research could encompass the development of privacy-preserving technologies, ethical guidelines for content creation, and strategies to mitigate potential societal challenges associated with widespread adoption.

Furthermore, the interdisciplinary nature of 360 AR in the cloud opens the door to collaborative research across fields such as human-computer interaction, computer vision, and cybersecurity. Researchers can explore novel ways to secure and authenticate user interactions within immersive environments, leveraging advancements in blockchain technology or biometric authentication. Collaborations between researchers, industry stakeholders, and policymakers could contribute to the establishment of standards and regulations that ensure the responsible and secure evolution of 360 AR technologies. Overall, future research endeavors in these areas have the potential to shape the trajectory of 360 AR in the cloud, driving innovation and addressing critical challenges to unlock the full potential of immersive mixed reality experiences.

## REFERENCES

[1] Balasubramanian K, Kunasekaran P, Konar R, Sakkthivel AM. Integration of Augmented Reality (AR) and Virtual Reality (VR) as Marketing Communications Channels in the Hospitality and Tourism Service Sector. InMarketing Communications and Brand Development in Emerging Markets Volume II: Insights for a Changing World 2022 May 25 (pp. 55-79). Cham: Springer International Publishing.

[2] Butt AU, Mahmood T, Saba T, Bahaj SO, Alamri FS, Iqbal MW, Khan AR. An Optimized Role-Based Access Control Using Trust Mechanism in E-Health Cloud Environment. IEEE Access. 2023 Nov 23.

[3] Chiang FK, Shang X, Qiao L. Augmented reality in vocational training: A systematic review of research and applications. Computers in Human Behavior. 2022 Apr 1;129:107125.

[4] 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.

[5] 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.

[6] 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.

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

[8] 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.

[9] Kharoub H, Lataifeh M, Ahmed N. 3D user interface design and usability for immersive VR. Applied sciences. 2019 Nov 13;9(22):4861.

  

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

[11] Mahmoud M, Rizou S, Panayides AS, Kantartzis NV, Karagiannidis GK, Lazaridis PI, Zaharis ZD. A Survey on Optimizing Mobile Delivery of 360° Videos: Edge Caching and Multicasting. IEEE Access. 2023 Jul 7.

[12] Nebeling M, Madier K. 360proto: Making interactive virtual reality & augmented reality prototypes from paper. InProceedings of the 2019 CHI Conference on Human Factors in Computing Systems 2019 May 2 (pp. 1-13).

[13] Osaki K, Oshima T, Sakamoto N, Aikawa T, Nishi Y, Kaneko T, Hatakeyama M, Yoshida M. Development of a Patrol System Using Augmented Reality and 360-Degree Camera. InAdvances in Condition Monitoring and Structural Health Monitoring: WCCM 2019 2021 Feb 3 (pp. 365-373). Singapore: Springer Singapore.

[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] Planas E, Martínez S, Brambilla M, Cabot J. Modeling and enforcing access control policies in conversational user interfaces. Software and Systems Modeling. 2023 Nov 22:1-20.

[16] Roopa D, Prabha R, Senthil GA. Revolutionizing education system with interactive augmented reality for quality education. Materials Today: Proceedings. 2021 Jan 1;46:3860-3.

[17] Sarkar A, Murray J, Dasari M, Zink M, Nahrstedt K. L3BOU: Low Latency, Low Bandwidth, Optimized Super-Resolution Backhaul for 360-Degree Video Streaming. In2021 IEEE International Symposium on Multimedia (ISM) 2021 Nov 29 (pp. 138-147). IEEE.

[18] Saxena UR, Alam T. Provisioning trust-oriented role-based access control for maintaining data integrity in cloud. International Journal of System Assurance Engineering and Management. 2023 Dec;14(6):2559-78.

[19] Syed TA, Siddiqui MS, Abdullah HB, Jan S, Namoun A, Alzahrani A, Nadeem A, Alkhodre AB. In-depth review of augmented reality: Tracking technologies, development tools, AR displays, collaborative AR, and security concerns. Sensors. 2022 Dec 23;23(1):146.

[20] Zhu Y, Min X, Zhu D, Zhai G, Yang X, Zhang W, Gu K, Zhou J. Toward visual behavior and attention understanding for augmented 360 degree videos. ACM Transactions on Multimedia Computing, Communications and Applications. 2023 Feb 17;19(2s):1-24.

[21] Zink M, Sitaraman R, Nahrstedt K. Scalable 360 video stream delivery: Challenges, solutions, and opportunities. Proceedings of the IEEE. 2019 Feb 17;107(4):639-50.

  