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

Volume – 08, Issue – 12, December 2023, PP – 10-19

Navigating the Confluence of 360-degree Mixed Reality and Edge Computing: A Comprehensive Review

Koffka Khan[1]

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

Abstract: As 360-degree Mixed Reality (MR) applications continue to redefine immersive experiences, the integration of edge computing introduces new dimensions to both performance and security considerations. This review paper delves into the multifaceted landscape of security challenges and solutions within the realm of 360-degree MR at the edge. We commence with an introduction to the foundational concepts of 360-degree MR technology, exploring its evolution and significance. Building upon this, we investigate the role of edge computing in enhancing the capabilities of 360-degree MR, emphasizing the need for a comprehensive security framework. The paper meticulously examines the distinct security challenges prevalent in 360-degree MR at the edge, ranging from data integrity and privacy concerns to authentication and authorization protocols. Special attention is devoted to the intricacies of securing network communications within the context of immersive environments. Drawing upon existing literature, we evaluate authentication mechanisms, discuss encryption practices, and highlight privacy-preserving strategies specific to 360-degree MR content. Furthermore, the review incorporates a comprehensive analysis of cyber security best practices, presenting recommendations for mitigating threats, incident response strategies, and recovery protocols. Real-world case studies illustrate practical implementations of security measures, providing valuable insights into successful deployments. The paper concludes by outlining future trends and research directions, recognizing the dynamic nature of security challenges in 360-degree MR at the edge. This comprehensive review not only synthesizes current knowledge on security in 360-degree MR but also serves as a roadmap for researchers, practitioners, and industry professionals seeking to fortify the integrity and privacy of immersive experiences in edge computing environments.

Keywords: 360-degree, Mixed Reality (MR), applications, edge, security

I. INTRODUCTION

In the dynamic landscape of immersive technologies, the convergence of 360-degree Mixed Reality (MR) with edge computing [14], [24], [11] heralds a transformative era in user experiences. Unlike traditional virtual reality, 360-degree MR seamlessly intertwines the virtual and physical realms, immersing users in a panoramic, interactive environment that mirrors reality. At the heart of this technological fusion lies the integration of edge computing, a paradigm that brings computational power and data processing closer to the point of interaction. This synergy not only enhances the responsiveness and efficiency of 360-degree MR applications but also introduces a host of security considerations essential for safeguarding the integrity of immersive experiences.

The significance of 360-degree MR transcends entertainment, finding applications across diverse sectors such as healthcare, education, video streaming [6], [7], [8], [9], [10], [12], gaming, and industry. Whether it is revolutionizing medical training through realistic simulations or augmenting educational content with immersive learning environments, the versatility of 360-degree MR is reshaping how we perceive and engage with information. As the adoption of these applications proliferates, so does the imperative to fortify the underlying infrastructure against security threats that could compromise user privacy, data integrity, and the seamless functionality of these immersive systems.

This paper embarks on a comprehensive exploration of the security landscape in 360-degree MR at the edge, recognizing the transformative potential of this amalgamation and acknowledging the critical need to address security concerns in tandem with technological advancements. As we delve into the intricate web of challenges and solutions within this domain, we navigate through the immersive realms of 360-degree MR to unravel the evolving dimensions of security that accompany this groundbreaking convergence.

This paper consists of eleven sections. In the "Introduction," the paper sets the stage by introducing the concept of 360-degree Mixed Reality (MR) at the edge, emphasizing its significance and diverse applications. It underscores the growing importance of addressing security concerns in this dynamic domain. The "Background and Overview of 360-degree Mixed Reality" section delves into the technology's fundamentals, tracing its

historical context and evolution while discussing the key components shaping 360-degree MR experiences. "Edge Computing in 360-degree Mixed Reality" defines edge computing, explores its benefits and challenges, and elaborates on how it enhances performance and reduces latency in MR applications. "Security Challenges in 360-degree Mixed Reality" identifies potential threats, delves into privacy concerns, and explores vulnerabilities in communication and data transfer. The "Authentication and Authorization in 360-degree MR" section reviews existing authentication methods, explores authorization mechanisms, and underscores the importance of identity management. "Data Integrity and Privacy Preservation" addresses issues related to data integrity, discusses privacy-preserving techniques, and explores encryption and secure data storage practices. "Network Security for 360-degree MR at the Edge" evaluates communication network security, discusses measures to secure data transmission, and explores the use of secure protocols. "Cybersecurity Best Practices" provides recommendations, discusses incident response strategies, and highlights industry standards. "Case Studies and Examples" presents real-world instances, analyzing successful implementations in diverse applications or industries. The "Future Trends and Research Directions" section explores emerging trends, identifies areas for future research, and anticipates advancements in security for 360-degree MR. In the "Conclusion," the paper summarizes key insights and findings, emphasizing the pivotal role of robust security measures in facilitating the widespread adoption of 360-degree MR at the edge.

II. BACKGROUND AND OVERVIEW OF 360-DEGREE MIXED REALITY

In the ever-evolving landscape of immersive technologies, 360-degree Mixed Reality (MR)[20], [15], [25], [19] stands as a pinnacle of innovation, seamlessly blending the virtual and physical worlds. To comprehend the intricacies of this transformative technology, it is essential to delve into its fundamental principles, historical evolution, and the intricate web of components that coalesce to create immersive 360-degree MR experiences.

At its core, 360-degree MR technology redefines the way users interact with digital content by enveloping them in a panoramic, all-encompassing environment. Unlike traditional virtual reality, which typically immerses users in computer-generated environments, 360-degree MR goes further by intertwining virtual elements with the real world. This immersive fusion is achieved through a combination of advanced hardware, sensors, and algorithms, allowing users to navigate and interact within a 360-degree field of view.

The roots of 360-degree MR can be traced back to the evolution of virtual reality and augmented reality. Early experiments in panoramic photography and stereoscopic imaging paved the way for immersive storytelling. Over the years, advancements in computing power, graphics rendering, and sensor technologies have propelled 360-degree MR into the mainstream. From its nascent stages as experimental prototypes to its current status as a transformative force across various industries, the evolution of 360-degree MR reflects a journey of continual innovation and refinement.

Creating immersive 360-degree MR experiences involves a symphony of key components and technologies. High-resolution cameras capture the surrounding environment, enabling the creation of seamless panoramic visuals. Advanced sensors, such as accelerometers and gyroscopes, track user movements and interactions, enhancing the sense of presence and realism. Meanwhile, powerful computing units process vast amounts of data in real-time, ensuring a responsive and dynamic user experience. The amalgamation of these components, coupled with innovative display technologies, facilitates the seamless integration of virtual and real-world elements, resulting in a truly immersive 360-degree MR encounter.

As we embark on this exploration of 360-degree MR, understanding the fundamentals, tracing its historical trajectory, and dissecting the technologies at play lay the foundation for a deeper appreciation of the security challenges and considerations inherent in this cutting-edge convergence with edge computing.

III. EDGE COMPUTING IN 360-DEGREE MIXED REALITY

In the realm of 360-degree Mixed Reality (MR), the integration of edge computing introduces a paradigm shift in the way computational processes are orchestrated. Edge computing, in this context, refers to the decentralization of computing resources, bringing data processing closer to the point of interaction—where the immersive magic of 360-degree MR unfolds. Unlike traditional cloud-based architectures, edge computing capitalizes on distributed nodes, often situated near the edge of the network, to handle processing tasks in close proximity to the end-user device.

The marriage of edge computing with 360-degree MR brings forth a myriad of benefits and, concurrently, novel challenges. One of the primary advantages lies in the reduction of latency. By processing data locally at the edge rather than relying on distant cloud servers, the lag between user input and system response diminishes significantly. This low-latency environment is crucial for maintaining the fluidity and realism integral to immersive MR experiences.

Furthermore, edge computing contributes to enhanced bandwidth efficiency. The localized processing of data means that only essential information is transmitted to the cloud, minimizing the strain on network resources. This not only results in a more responsive MR system but also optimizes bandwidth usage, a critical consideration in scenarios where network congestion may impede the seamless delivery of 360-degree content.

However, the adoption of edge computing in 360-degree MR is not without its challenges. The distribution of computing tasks across a decentralized network necessitates robust security measures to safeguard sensitive user data and ensure the integrity of immersive content. Moreover, managing the heterogeneity of edge devices and orchestrating seamless collaboration among them pose intricate challenges that demand careful consideration.

At the core of the synergy between edge computing and 360-degree MR lies the tangible improvement in performance and latency reduction. The proximity of computational resources to the end-user device translates to faster data processing and, consequently, reduced latency in rendering immersive content. This not only heightens the sense of presence for users but also enables more dynamic and responsive interactions within the 360-degree environment.

The optimization of performance is particularly pronounced in scenarios where real-time responsiveness is critical, such as gaming, training simulations, or interactive educational content. By harnessing the power of edge computing, 360-degree MR applications achieve a level of immediacy that is foundational to delivering an authentic and captivating user experience.

As we navigate the convergence of edge computing with 360-degree MR, it becomes evident that the benefits are intertwined with unique challenges, underscoring the importance of a nuanced approach to security in this dynamic and transformative landscape.

IV. SECURITY CHALLENGES IN 360-DEGREE MIXED REALITY

The seamless integration of 360-degree Mixed Reality (MR) with edge computing presents a unique set of security challenges [1], [4], [16], [5], necessitating a comprehensive examination of potential threats specific to this immersive landscape. One prominent concern lies in the vulnerability of the devices at the edge to cyber-attacks and unauthorized access. As 360-degree MR systems rely on a network of interconnected devices, any compromise in the security of individual components could have cascading effects, compromising the integrity of the entire immersive experience.

Furthermore, the immersive nature of 360-degree MR creates opportunities for novel cyber threats, including spatially aware attacks that target the physical environment in which users are immersed. Understanding and mitigating these threats are imperative to fortify the security posture of 360-degree MR at the edge.

The very essence of 360-degree MR lies in the immersion of users in a synthesized environment, often requiring the collection and processing of highly personal and sensitive data. Privacy concerns emerge as a paramount challenge in this context, as the immersive data generated by user interactions may include spatial mapping, biometric data, and behavioral patterns. The edge computing paradigm exacerbates these concerns, as the processing of such intimate data occurs in close proximity to the end-user device.

Navigating the delicate balance between providing immersive experiences and preserving user privacy requires meticulous attention to data governance, consent mechanisms, and robust encryption protocols. Addressing privacy concerns is not only a regulatory imperative but also crucial for fostering user trust and encouraging widespread adoption of 360-degree MR technologies.

The interconnected nature of devices at the edge introduces vulnerabilities in communication channels and data transfer protocols, raising concerns about the confidentiality and integrity of information exchanged between edge devices. As data traverses the network between sensors, processors, and display units, it becomes susceptible to eavesdropping, interception, and unauthorized access.

Mitigating these vulnerabilities requires the implementation of secure communication protocols, encryption mechanisms, and authentication procedures. Additionally, the heterogeneity of devices within the 360-degree MR ecosystem necessitates standardized security practices to ensure seamless and secure data exchange, fostering a resilient and interconnected environment.

In this complex interplay between immersive experiences, edge computing, and security, understanding and addressing these challenges are imperative. As we delve into the nuances of security threats, privacy considerations, and communication vulnerabilities, a holistic approach to fortifying 360-degree MR at the edge emerges as a prerequisite for realizing the full potential of this transformative convergence.

V. AUTHENTICATION AND AUTHORIZATION IN 360-DEGREE MR

As 360-degree Mixed Reality (MR) environments continue to redefine user interactions, the need for robust authentication mechanisms [17], [22], [13], [21] becomes paramount. Reviewing existing authentication methods for users engaging with 360-degree MR systems reveals a diverse landscape of techniques. Traditional username-password combinations, biometric authentication, and multifactor authentication are prevalent, each with its advantages and challenges.

Biometric authentication, such as facial recognition or fingerprint scanning, adds an extra layer of security by uniquely identifying users based on physical characteristics. However, concerns regarding privacy and data protection must be carefully addressed. Multifactor authentication, combining something the user knows (e.g., a password) with something the user possesses (e.g., a mobile device), provides an additional security layer. Evaluating the effectiveness of these methods within the context of 360-degree MR is essential to strike a balance between security and user experience.

Beyond authentication, effective authorization mechanisms are critical to ensuring secure access to 360-degree MR content and functionalities. Authorization involves defining and enforcing policies that dictate what actions users are allowed to perform within the MR environment. Role-based access control (RBAC), attribute-based access control (ABAC), and discretionary access control (DAC) are among the authorization models considered.

In the context of 360-degree MR, where user interactions can range from immersive educational experiences to sensitive corporate simulations, tailoring authorization mechanisms becomes crucial. RBAC may be suitable for scenarios where predefined roles dictate access levels, while ABAC allows for more dynamic access control based on user attributes. Striking a balance between granularity and manageability is key to implementing effective authorization in the diverse landscape of 360-degree MR applications.

Identity management emerges as a linchpin in establishing a secure and user-friendly 360-degree MR environment. The dynamic nature of MR interactions, coupled with the distributed processing paradigm of edge computing, underscores the importance of seamlessly managing user identities. Robust identity management not only ensures that users are who they claim to be (authentication) but also governs what actions they are allowed to perform (authorization).

In a 360-degree MR environment, effective identity management enhances user experience by providing personalized content and settings while safeguarding sensitive data. This involves establishing and maintaining a user's digital identity securely across devices and sessions. Solutions that incorporate federated identity management and single sign-on mechanisms contribute to a cohesive and secure user experience within the immersive realms of 360-degree MR.

In navigating the intricate interplay of authentication, authorization, and identity management, a nuanced approach is essential to strike a balance between security, usability, and the unique demands of 360-degree MR applications.

VI. DATA INTEGRITY AND PRIVACY PRESERVATION

In the immersive landscape of 360-degree Mixed Reality (MR), maintaining the integrity of data throughout its lifecycle is fundamental to preserving the authenticity and coherence of user experiences. Challenges arise in the creation, storage, and transmission phases, where the fidelity of 360-degree MR content is paramount. Ensuring data integrity begins at the point of content creation, where calibration and synchronization of multiple sensors must be precise to avoid discrepancies[21][3], [2], [23] in spatial mapping and rendering.

During storage, robust file management practices, version control, and error-checking mechanisms are essential to prevent corruption or loss of critical data. Additionally, in the transmission phase, network protocols must be resilient to packet loss and latency, guaranteeing that the immersive experience faithfully reflects the creator's intent. Addressing these challenges demands a comprehensive approach to data integrity that spans the entire lifecycle of 360-degree MR content.

360-degree MR environments inherently involve the collection of sensitive user data, necessitating a concerted effort to implement privacy-preserving techniques. As users interact within immersive spaces, spatial mapping, gaze tracking, and behavioral data are generated, raising concerns about the potential misuse of personal information. Anonymization and pseudonymization techniques are crucial for dissociating user identities from collected data, safeguarding individual privacy.

In the design and development of 360-degree MR applications, adopting a privacy-by-design approach becomes imperative. This involves implementing features such as user consent mechanisms, granular control over data sharing, and transparent privacy policies. Moreover, techniques like differential privacy can be explored to add noise to data, preventing the identification of individuals while still allowing for meaningful

insights. By integrating these privacy-preserving measures, 360-degree MR developers can navigate the delicate balance between delivering immersive experiences and respecting user privacy.

The secure handling of data in 360-degree MR extends to encryption and storage practices, safeguarding information from unauthorized access and potential breaches. Encryption of data during transmission ensures that sensitive information remains confidential while traversing networks. Protocols such as Transport Layer Security (TLS) play a pivotal role in securing communication channels between edge devices, preventing eavesdropping and tampering.

In the realm of storage, adopting secure data storage practices involves encryption at rest and access controls. Encryption at rest ensures that data stored on devices or servers remains unreadable without the appropriate decryption keys. Implementing access controls based on the principle of least privilege restricts user and system access to sensitive data, minimizing the risk of unauthorized manipulation or exposure.

As 360-degree MR content evolves, the implementation of encryption and secure storage practices becomes not only a technological necessity but also a foundational element in building user trust. Striking the right balance between data security and user experience is pivotal to fostering a resilient and privacy-conscious ecosystem within the immersive realms of 360-degree MR.

VII. NETWORK SECURITY FOR 360-DEGREE MR AT THE EDGE

The interconnected nature of edge devices in 360-degree Mixed Reality (MR) setups introduces a critical dimension to network security [18]. Evaluating the security of communication networks is paramount to safeguarding the integrity and confidentiality of data in transit. As 360-degree MR applications heavily rely on seamless communication between sensors, processors, and display units, vulnerabilities in network architecture could compromise the immersive experience and expose sensitive information to potential threats.

Assessing the robustness of network security involves scrutinizing the architecture for potential weak points, ensuring that communication channels are resistant to various cyber threats. Understanding the specific requirements of 360-degree MR setups is crucial to designing networks that can withstand potential attacks and provide a secure foundation for data transmission.

Securing data transmission is a focal point in the network security paradigm for 360-degree MR at the edge. Measures must be implemented to protect data as it traverses the network, minimizing the risk of interception or tampering. Encryption emerges as a fundamental technique, ensuring that data remains confidential and integral during transmission.

Implementing end-to-end encryption, where data is encrypted on the sender's device and decrypted only on the recipient's device, mitigates the risk of eavesdropping. Additionally, techniques such as tunneling through virtual private networks (VPNs) can add an extra layer of protection, creating a secure and private communication channel between edge devices. By adopting these measures, 360-degree MR systems can ensure that the immersive content and user data remain safeguarded against potential malicious actors on the network.

The choice of secure protocols and technologies is instrumental in fortifying network communication within 360-degree MR setups. Secure communication protocols such as HTTPS (Hypertext Transfer Protocol Secure) or MQTT (Message Queuing Telemetry Transport) enhance the confidentiality and integrity of data exchanged between devices. These protocols, coupled with secure socket layers (SSL) or transport layer security (TLS), establish encrypted connections, protecting against eavesdropping and unauthorized access.

In the context of edge computing, where devices may have diverse capabilities and communication requirements, adopting standardized secure protocols becomes crucial for interoperability and resilience. Exploring emerging technologies such as blockchain for secure and transparent transactions in decentralized networks could also contribute to enhancing the overall security posture of 360-degree MR at the edge.

By evaluating communication networks, implementing robust measures for data transmission security, and leveraging secure protocols and technologies, 360-degree MR systems can establish a secure foundation for immersive experiences at the edge. This comprehensive approach to network security is integral to preserving the confidentiality, integrity, and availability of data in the dynamic and interconnected world of 360-degree MR.

VIII. CYBERSECURITY BEST PRACTICES

Securing 360-degree Mixed Reality (MR) at the edge demands a proactive and multifaceted approach.

Here are several recommendations and best practices to fortify the cybersecurity posture:

- Device Security: Ensure that all edge devices, including sensors, processors, and display units, are equipped with the latest security updates and patches. Implement device-level security measures such as secure boot, device attestation, and hardware-based encryption to protect against unauthorized

access.

- Network Segmentation: Employ robust network segmentation strategies to isolate different components within the 360-degree MR ecosystem. This prevents lateral movement of attackers and limits the impact of potential breaches.
- User Authentication: Implement strong and adaptive user authentication mechanisms. Multifactor authentication, biometric verification, and token-based access control enhance user identity validation and protect against unauthorized access.
- Data Encryption: Enforce end-to-end encryption for data in transit and at rest. Utilize strong encryption algorithms and regularly update encryption keys to safeguard sensitive information from eavesdropping and unauthorized access.
- Regular Audits and Assessments: Conduct regular security audits and vulnerability assessments to identify and remediate potential weaknesses in the 360-degree MR system. This includes both hardware and software components.

Strategies for Threat Detection, Incident Response, and Recovery:

- Continuous Monitoring: Implement continuous monitoring solutions to detect abnormal activities or potential security breaches. This includes monitoring network traffic, user behaviors, and system logs to identify anomalies indicative of a cyber threat.
- Incident Response Plan: Develop a comprehensive incident response plan that outlines the steps to be taken in the event of a security incident. Define roles and responsibilities, establish communication protocols, and conduct regular drills to ensure the effectiveness of the plan.
- Threat Intelligence Integration: Integrate threat intelligence feeds to stay informed about emerging threats and vulnerabilities relevant to 360-degree MR technologies. This proactive approach enhances the ability to preemptively defend against evolving cyber threats.
- Automated Response Mechanisms: Implement automated response mechanisms for certain types of security incidents. Automated responses can help mitigate the impact of an incident in real-time and reduce the reliance on manual intervention.
- Backup and Recovery: Regularly backup critical data and develop a robust data recovery strategy. This ensures that, in the event of a security incident, data can be restored, minimizing downtime and potential data loss.

Industry Standards and Guidelines:

- ISO/IEC 27001: Adhere to the ISO/IEC 27001 standard for information security management systems. This internationally recognized standard provides a framework for establishing, implementing, maintaining, and continually improving an organization's information security management system.
- NIST Cybersecurity Framework: Align cybersecurity practices with the NIST Cybersecurity Framework, which provides a risk-based approach to managing and improving the cybersecurity posture of organizations. The framework emphasizes functions such as Identify, Protect, Detect, Respond, and Recover.
- Immersive Technology Guidelines: Stay abreast of industry-specific guidelines and best practices for immersive technologies. Organizations such as the XR Association and Immersive Digital Experiences Alliance (IDEA) may release standards relevant to the security of 360-degree MR applications.

By adopting these cybersecurity best practices, organizations can navigate the dynamic and interconnected landscape of 360-degree MR at the edge with resilience and confidence, safeguarding both the integrity of immersive experiences and the privacy of user data.

IX. CASE STUDIES AND EXAMPLES

Here are Real-world Examples Illustrating Security Challenges and Solutions:

Healthcare Simulations:

- Challenge: In a 360-degree MR healthcare simulation environment, the challenge is to secure patient data and maintain the privacy of sensitive medical information.
- Solution: Implementing end-to-end encryption for data transmission, adopting secure user authentication for healthcare professionals, and employing anonymization techniques to dissociate

patient identities from simulation data.

Corporate Training Programs:

- Challenge: Security concerns arise in 360-degree MR corporate training programs where proprietary business data is involved, necessitating protection against industrial espionage or unauthorized access.
- Solution: Employing access controls based on roles and responsibilities, implementing secure network communication protocols, and utilizing encrypted storage for training materials and user progress data.

Here are Analysis of Successful Implementations:
Education and Virtual Classrooms:

- Implementation: A university's deployment of 360-degree MR for virtual classrooms involves secure user authentication for students and educators, ensuring access only to authorized participants.
- Success Analysis: By adopting role-based access controls, the university ensures that students can access educational content while educators have additional privileges for content creation and management. Regular security audits and updates contribute to a resilient educational environment.

Defense and Military Training:

- Implementation: A defense contractor utilizes 360-degree MR for military training simulations. Security measures include encrypted communication channels, secure user authentication for trainees, and restricted access to classified scenarios.
- Success Analysis: The implementation has proven successful in creating realistic training environments while maintaining the confidentiality of sensitive military tactics. Regular security assessments ensure the integrity of the training programs.

Immersive Healthcare Consultations:

- Implementation: A healthcare provider adopts 360-degree MR for immersive telemedicine consultations. Security measures involve encrypted video communication, secure storage of patient health records, and stringent user authentication for healthcare professionals.
- Success Analysis: The implementation enhances patient-doctor interactions while safeguarding sensitive medical information. Compliance with healthcare data protection regulations ensures a secure and compliant telemedicine platform.

These case studies highlight the diverse applications of 360-degree MR and the corresponding security challenges and solutions within specific industries. Successful implementations showcase the adaptability of security measures to meet the unique requirements of each use case, emphasizing the importance of a tailored and comprehensive approach to security in the dynamic landscape of immersive technologies.

X. FUTURE TRENDS AND RESEARCH DIRECTIONS

Here are Emerging Trends and Advancements:

1. **Edge-based AI for Security:**
   - **Trend:** The integration of edge-based artificial intelligence (AI) for security purposes is emerging as a trend. Machine learning algorithms deployed at the edge can enhance threat detection capabilities and mitigate security risks in real-time.
   - **Advancement:** Research is underway to develop AI models capable of identifying anomalous patterns in user behavior, detecting potential cyber threats, and dynamically adapting security measures in response to evolving risks.

2. **Blockchain for Decentralized Security:**
   - **Trend:** The use of blockchain technology for decentralized security in 360-degree MR is gaining traction. Blockchain's distributed ledger can provide a secure and transparent framework for managing access control, data integrity, and identity verification.
   - **Advancement:** Ongoing research explores the implementation of blockchain-based smart contracts to enforce secure transactions and permissions within the 360-degree MR ecosystem. This includes ensuring the integrity of content creation and distribution.

Here are Areas for Future Research and Development:

1. **Dynamic Threat Modeling in Immersive Environments:**
   - **Research Direction:** Future research should focus on dynamic threat modeling specific to immersive environments. This involves continuously assessing the evolving threat landscape for 360-degree MR at the edge and adapting security measures accordingly.
   - **Development:** Developing threat modeling frameworks that account for the unique challenges posed by spatially aware attacks and novel cyber threats in immersive scenarios. This includes exploring adaptive security policies and intrusion detection systems tailored to 360-degree MR.

2. **Quantum-safe Cryptography for Immersive Technologies:**
   - **Research Direction:** As quantum computing advancements pose a potential threat to traditional cryptographic methods, future research should explore quantum-safe cryptography for 360-degree MR.
   - **Development:** Investigating and developing cryptographic algorithms resistant to quantum attacks to ensure the long-term security of immersive environments. This includes evaluating the feasibility and performance of quantum-resistant encryption in real-time 360-degree MR applications.

3. **Usable Security Interfaces for MR Users:**
   - **Research Direction:** Enhancing the usability of security interfaces for users within immersive environments is a critical research area.
   - **Development:** Investigating user-friendly authentication methods, intuitive privacy controls, and immersive visualizations of security status. This includes developing interfaces that provide users with a clear understanding of the security measures in place and empower them to make informed decisions about their privacy and data.

4. **Standardization of Security Protocols:**
   - **Research Direction:** Standardizing security protocols specific to 360-degree MR at the edge is essential for interoperability and a unified security framework.
   - **Development:** Collaborative efforts to establish industry standards for secure communication, authentication, and data protection in 360-degree MR. This involves engaging with stakeholders, industry alliances, and standardization bodies to create guidelines that ensure consistent and robust security practices across immersive applications.

As 360-degree MR at the edge continues to evolve, future research and development efforts should be directed towards proactive security measures that align with emerging trends, addressing novel challenges and opportunities in the immersive technology landscape. By exploring these research directions, the field can stay ahead of potential security threats and continue to foster a secure and immersive user experience.

XI. CONCLUSION

In conclusion, this comprehensive review has delved into the intricate intersection of 360-degree Mixed Reality (MR) and edge computing, shedding light on the evolving security landscape within this transformative convergence. The exploration of key components, security challenges, and best practices has unearthed crucial insights that lay the groundwork for understanding and fortifying the immersive realms of 360-degree MR at the edge.

From the fundamentals of 360-degree MR technology to the integration of edge computing and the associated security challenges, the review has traversed the multidimensional aspects of this dynamic landscape. Authentication and authorization mechanisms, data integrity and privacy preservation techniques, network security considerations, and cybersecurity best practices have been scrutinized to provide a holistic view of the intricate interplay between immersive experiences and security requirements.

The transformative potential of 360-degree MR at the edge is undeniable, permeating diverse sectors and redefining user experiences. However, this transformative power comes hand in hand with the responsibility to fortify the underlying infrastructure against an array of security threats. The importance of robust security measures cannot be overstated, as they form the linchpin for fostering user trust, ensuring data integrity, and enabling the widespread adoption of 360-degree MR technologies.

In an era where immersive technologies are poised to reshape how we interact with information and environments, the success and acceptance of 360-degree MR hinge on the assurance of a secure and resilient ecosystem. From healthcare simulations to corporate training programs, the case studies and examples

highlighted the versatility of 360-degree MR applications and the critical role security measures play in diverse industry contexts.

As we gaze into the future of 360-degree MR at the edge, emerging trends in edge-based AI for security and the utilization of blockchain for decentralized security showcase the ongoing evolution of protective measures. Dynamic threat modeling, quantum-safe cryptography, usable security interfaces, and standardization efforts beckon researchers and industry practitioners to chart the course for the next phase of security advancements in immersive technologies.

In the ever-evolving landscape of 360-degree MR, one resounding truth remains — robust security is not merely a safeguard but a catalyst for innovation, trust, and the realization of the full transformative potential of immersive experiences. As the technology continues to unfold, a steadfast commitment to security will pave the way for a future where 360-degree MR at the edge becomes an integral and secure facet of our interconnected digital world.

REFERENCES

[1] Cho H, Komar ML, Lindlbauer D. Reality Replay: Detecting and Replaying Temporal Changes In Situ Using Mixed Reality. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 2023 Sep 27;7(3):1-25.

[2] David-John B, Butler K, Jain E. For your eyes only: Privacy-preserving eye-tracking datasets. In2022 Symposium on Eye Tracking Research and Applications 2022 Jun 8 (pp. 1-6).

[3] David-John B, Hosfelt D, Butler K, Jain E. A privacy-preserving approach to streaming eye-tracking data. IEEE Transactions on Visualization and Computer Graphics. 2021 Mar 22;27(5):2555-65.

[4] Huang JC. From Building Information Modeling to Extended Reality. Industry 4.0 for the Built Environment: Methodologies, Technologies and Skills. 2021 Dec 3:471-93.

[5] Isa MF, Ab Rahim NZ, Fathi MS. Review of remote audit in occupational safety and health management system through the mixed-reality spectrum. In2021 7th International Conference on Research and Innovation in Information Systems (ICRIIS) 2021 Oct 25 (pp. 1-6). IEEE.

[6] Khan K, Goodridge W. Future DASH applications: A survey. International Journal of Advanced Networking and Applications. 2018 Sep 1;10(2):3758-64.

[7] Khan K, Goodridge W. Markov Decision Processes for bitrate harmony in adaptive video streaming. In2017 Future Technologies Conference (FTC), Vancouver, Canada, unpublished.

[8] 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.

[9] Khan K, Goodridge W. QoE in DASH. International Journal of Advanced Networking and Applications. 2018;9(4):3515-22.

[10] Khan K, Goodridge W. Server-based and network-assisted solutions for adaptive video streaming. International Journal of Advanced Networking and Applications. 2017 Nov 1;9(3):3432-42.

[11] Kim HJ. TeleGate: Multi-user Semi-teleportation for Remote Collaboration in Mixed Reality 360-Videos (Doctoral dissertation, Open Access Te Herenga Waka-Victoria University of Wellington).

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

[13] Lee L, Nisar H, Roberts J, Blackford J, Kesavadas TK. Face and Content Validation of Food Safety Training in Virtual Reality (VR). In2022 IEEE 10th International Conference on Serious Games and Applications for Health (SeGAH) 2022 Aug 10 (pp. 1-5). IEEE.

[14] Li P, Chen F, Wang R, Hoang T, Pan L. InstaVarjoLive: An Edge-Assisted 360 Degree Video Live Streaming for Virtual Reality Testbed. In2022 18th International Conference on Mobility, Sensing and Networking (MSN) 2022 Dec 14 (pp. 609-613). IEEE.

[15] Maas MJ, Hughes JM. Virtual, augmented and mixed reality in K–12 education: A review of the literature. Technology, Pedagogy and Education. 2020 Mar 14;29(2):231-49.

[16] McGill M, Williamson J, Ng A, Pollick F, Brewster S. Challenges in passenger use of mixed reality headsets in cars and other transportation. Virtual Reality. 2020 Dec; 24:583-603.

[17] Saad A, Liebers J, Gruenefeld U, Alt F, Schneegass S. Understanding Bystanders' tendency to shoulder surf smartphones using 360-degree videos in virtual reality. In Proceedings of the 23rd International Conference on Mobile Human-Computer Interaction 2021 Sep 27 (pp. 1-8).

[18] Soldatos J. A 360-degree view of IoT technologies. Artech House; 2020 Dec 31.

[19] Tarko J, Tompkin J, Richardt C. Omnimr: Omni directional 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.

[20] Teo T, Lawrence L, Lee GA, Billinghurst M, Adcock M. Mixed reality remote collaboration combining 360 video and 3d reconstruction. In Proceedings of the 2019 CHI conference on human factors in computing systems 2019 May 2 (pp. 1-14).

[21] Vercelloni J, Peppinck J, Santos-Fernandez E, McBain M, Heron G, Dodgen T, Peterson EE, Mengersen K. Connecting virtual reality and ecology: a new tool to run seamless immersive experiments in R. PeerJ Computer Science. 2021 Jun 1; 7:e544.

[22] Viswanathan K, Yazdinejad A. Security considerations for virtual reality systems. arXiv preprint arXiv:2201.02563. 2022 Jan 7.

[23] Wierzbowski M, Pochwatko G, Borkiewicz P, Cnotkowski D, Pabiś-Orzeszyna M, Kobyliński P. Behavioural Biometrics in Virtual Reality: To What Extent Can We Identify a Person Based Solely on How They Watch 360-Degree Videos?. In2022 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct) 2022 Oct 17 (pp. 417-422). IEEE.

[24] Zhu Y, Fukuda T, Yabuki N. A Mixed Reality Design System for Interior Renovation: Inpainting With 360-Degree Live Streaming and Generative Adversarial Networks After Removal.

[25] Zhu Y, Fukuda T, Yabuki N. A Mixed Reality Design System for Interior Renovation: Inpainting With 360-Degree Live Streaming and Generative Adversarial Networks After Removal.

