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

Volume – 08, Issue – 12, December 2023, PP – 92-98

Beyond Pixels: Ensuring Security in Cloud-Based 360 Virtual Reality Streaming

Koffka Khan[1]

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

Abstract: Virtual Reality (VR) has witnessed unprecedented growth with the integration of 360 video streaming, offering immersive experiences to users. As this technology evolves, the demand for secure and efficient content delivery becomes paramount, especially within the framework of cloud computing. This review paper explores the challenges and solutions associated with secure 360 video streaming in VR environments hosted on cloud platforms. We delve into the unique security considerations posed by the fusion of VR and cloud computing, addressing issues such as data integrity, confidentiality, and user authentication. The paper examines existing transmission protocols, encryption techniques, and access control mechanisms tailored for the secure delivery of 360 video content. Furthermore, it explores the integration of Content Delivery Networks (CDNs) in optimizing performance and security. Through real-world case studies and implementation examples, we highlight successful instances of secure 360 video streaming within virtual reality, drawing insights and lessons for practitioners and researchers. Additionally, the paper identifies emerging trends and proposes future research directions to foster the continued advancement of secure VR content delivery in cloud environments. This comprehensive review serves as a valuable resource for professionals, researchers, and enthusiasts navigating the intersection of virtual reality, cloud computing, and secure content streaming.

Keywords: Virtual Reality (VR), 360-degree video streaming, cloud computing, security

I. INTRODUCTION

360 video streaming in virtual reality (VR) [13], [9], [30], [6] represents a revolutionary form of immersive content delivery, allowing users to explore and interact with their surroundings in a 360-degree environment. This technology has found applications in various domains, from gaming and entertainment to education and training. Unlike traditional video streaming [17], [19], [20], [22], 360 VR video enables users to navigate the virtual space by adjusting their perspective, creating a more engaging and lifelike experience.

As the demand for VR experiences continues to rise, the importance of secure streaming in cloud-based VR applications becomes paramount. Cloud-based streaming offers scalability, accessibility, and cost-effectiveness, making it an attractive solution for delivering VR content to a global audience. However, ensuring the security and integrity of the streamed content is critical to protect user privacy, prevent unauthorized access, and maintain the overall quality of the VR experience. This includes implementing robust encryption protocols, secure authentication mechanisms, and content delivery networks (CDNs) with advanced security features.

In the realm of secure 360 VR video streaming, several challenges and opportunities emerge. One major challenge is the need for high bandwidth and low latency to deliver seamless and lag-free experiences. The large file sizes associated with 360-degree videos demand efficient compression techniques and optimized streaming protocols. Additionally, ensuring data privacy and protection against potential cyber threats is crucial, given the sensitive nature of VR content. Opportunities lie in the development of innovative security solutions, such as blockchain-based authentication and watermarking technologies, to enhance content protection. As the technology continues to evolve, collaboration between industry stakeholders, including content creators, streaming platforms, and cybersecurity experts, will be essential to address these challenges and unlock the full potential of secure 360 VR video streaming in the cloud.

This review paper comprehensively examines the landscape of secure 360 video streaming in virtual reality (VR) within a cloud environment. Starting with an overview of the evolution of VR and its integration with 360 video streaming, the paper emphasizes the unique security challenges associated with this convergence. It explores the role of cloud computing in supporting VR applications and discusses the specific challenges and opportunities of secure content delivery. The review encompasses a thorough analysis of transmission protocols, encryption techniques, and access control mechanisms tailored to the VR context. Real-world case studies and implementation examples showcase successful instances of secure 360 video streaming in the cloud, providing practical insights and lessons. The integration of Content Delivery Networks (CDNs) for optimizing performance and security is also explored. The paper concludes by identifying emerging trends and

proposing future research directions to propel the advancement of secure VR content delivery, offering a comprehensive resource for professionals and researchers navigating this dynamic intersection.

II. BACKGROUND

The evolution of virtual reality (VR) [29], [28] has been a fascinating journey, transforming the way users engage with digital content. Initially rooted in gaming and simulations, VR has evolved to encompass diverse fields such as education, healthcare, and entertainment. One significant enhancement to the VR experience is the integration of 360 video streaming. This technology allows users to immerse themselves in a complete 360-degree environment, fostering a sense of presence and interactivity. By capturing and streaming content from all directions, 360 video adds a new layer of realism to virtual experiences, enabling users to explore and interact with their surroundings as if they were physically present. This evolution represents a paradigm shift from traditional flat-screen experiences to a more immersive and engaging form of content consumption.

The significance of cloud computing in enhancing VR experiences cannot be overstated. Cloud-based platforms provide the infrastructure needed to deliver VR content efficiently and at scale. As VR applications, particularly those involving 360 video streaming, demand substantial computational resources and storage, the cloud offers a flexible and scalable solution. Cloud computing enables the seamless distribution of VR content to a global audience, allowing users to access immersive experiences without the need for powerful local hardware. Moreover, cloud-based VR applications benefit from the latest advancements in processing power and network capabilities, contributing to enhanced graphics, reduced latency, and an overall improvement in the quality of the VR experience.

In the landscape of 360 video streaming technologies and platforms[33], several solutions have emerged to meet the growing demand for immersive content delivery. Major players in the industry, such as YouTube and Facebook, have integrated support for 360-degree videos, allowing users to upload and stream immersive content. Additionally, specialized platforms like Vimeo and VeeR VR have focused on providing high-quality 360 video streaming services. These platforms often leverage adaptive streaming techniques, where the video quality is dynamically adjusted based on the viewer's internet connection speed, ensuring a smooth and uninterrupted experience. As the popularity of 360 video streaming continues to rise, technological advancements, standardization efforts, and innovations in content creation are expected to further shape the landscape of this immersive and dynamic form of virtual reality.

III. SECURITY CHALLENGES IN VR STREAMING

Secure 360 virtual reality (VR) video streaming [11], [23], [31], [25], [7] in the cloud presents a set of unique security challenges that stem from the immersive and interactive nature of the content. One of the primary concerns is ensuring the integrity of the 360-degree video data. As users navigate through the virtual environment, any compromise in data integrity can lead to distortions in the visual representation, disrupting the immersive experience. To address this, robust data integrity mechanisms, such as error-checking codes and cryptographic hashing, are crucial to detect and mitigate any unauthorized alterations to the streamed content.

Confidentiality is another critical aspect of secure VR video streaming, particularly considering the personal and sensitive nature of the virtual experiences. Protecting user data and the content itself from unauthorized access is imperative. Encryption protocols, such as Transport Layer Security (TLS) for data in transit and storage encryption for data at rest, play a pivotal role in safeguarding the confidentiality of 360 VR video content. Additionally, the implementation of secure authentication mechanisms ensures that only authorized users have access to the VR streams, mitigating the risk of unauthorized viewing or data manipulation.

Authentication and authorization are essential components of securing 360 VR video streaming in the cloud. Effective authentication verifies the identity of users, ensuring that only legitimate individuals can access the VR content. Multi-factor authentication and biometric verification can enhance the level of identity assurance in the VR context. Authorization mechanisms dictate the level of access granted to authenticated users, preventing unauthorized interactions with sensitive content. Fine-grained access controls based on user roles and permissions are vital to maintaining a secure and controlled VR streaming environment.

In conclusion, addressing the unique security challenges associated with 360 VR video streaming in the cloud requires a comprehensive approach that encompasses data integrity, confidentiality, authentication, and authorization. Implementing state-of-the-art encryption, robust authentication protocols, and precise access controls will contribute to a secure and trustworthy environment for users to enjoy immersive and interactive virtual reality experiences.

IV. CLOUD COMPUTING AND VR INTEGRATION

Cloud computing [3], [2], [27], [1] plays a pivotal role in supporting virtual reality (VR) applications, particularly in the context of 360 video streaming. The integration of cloud services provides a scalable and flexible infrastructure that addresses the resource-intensive nature of VR content delivery. In the case of 360 video streaming, the cloud enables the storage and processing of vast amounts of data associated with capturing and rendering immersive, high-resolution video. The scalability of cloud resources allows VR applications to cater to a global audience, ensuring that users can access high-quality and interactive 360-degree experiences without relying on localized, powerful hardware. Cloud platforms also facilitate the efficient distribution of VR content, optimizing streaming performance and reducing latency, essential for delivering a seamless and immersive user experience.

While leveraging cloud services for VR content delivery offers numerous advantages, there are also potential drawbacks to consider. One notable advantage is cost-effectiveness, as cloud-based models allow businesses to pay for the resources they consume, avoiding the need for substantial upfront investments in infrastructure. Additionally, cloud services provide flexibility, enabling rapid deployment and updates to VR applications. However, potential drawbacks include concerns related to data privacy and security. Storing sensitive VR content in the cloud requires robust measures to protect against unauthorized access, ensuring the confidentiality and integrity of user experiences. Moreover, reliance on the internet for content delivery introduces the risk of latency, impacting the real-time interactivity crucial for VR applications. Striking a balance between the advantages and drawbacks of leveraging cloud services is essential for maximizing the potential of secure and efficient 360 VR video streaming in the cloud.

V. SECURE TRANSMISSION PROTOCOLS

In the realm of secure 360 virtual reality (VR) video streaming in the cloud[8], [10], [32], [14], [14], the choice of transmission protocols plays a critical role in ensuring a seamless and secure user experience. Existing and emerging protocols cater to the unique requirements of VR content, including low latency, high bandwidth, and robust security measures. One widely adopted protocol is the HTTP Adaptive Streaming (HAS) family, such as HTTP Live Streaming (HLS) and Dynamic Adaptive Streaming over HTTP (DASH)[18], [15], [16]. These protocols allow the adaptive streaming of 360 VR video, dynamically adjusting the quality and resolution based on the viewer's network conditions. While efficient in managing bandwidth, they may introduce latency due to the segmentation of video files.

Emerging protocols like the Common Media Application Format (CMAF)[5] aim to address latency issues by combining the benefits of HLS and DASH. CMAF achieves low-latency streaming by using a single format for both protocols, streamlining the delivery process. Additionally, Web Real-Time Communication (WebRTC) [4] has gained traction for its real-time capabilities, making it suitable for interactive VR applications. WebRTC enables peer-to-peer communication, reducing latency and enhancing the overall responsiveness of VR content. However, security considerations are crucial, and WebRTC implementations often require additional measures to ensure the confidentiality and integrity of the transmitted VR data.

Protocols such as Secure Reliable Transport (SRT) focus on enhancing security during content delivery. SRT is designed to provide secure, low-latency video streaming over unpredictable networks. It incorporates features like encryption and error correction to ensure the secure and reliable transmission of VR content. In the context of VR, where immersive experiences demand real-time interactions and high-quality visuals, a balance between low latency, high bandwidth, and robust security is paramount. As the landscape of VR technology evolves, ongoing advancements in transmission protocols will likely address these requirements more comprehensively, further optimizing the secure streaming of 360 VR video in cloud-based environments.

VI. ENCRYPTION TECHNIQUES

Securing 360 virtual reality (VR) video streams in the cloud involves the implementation of robust encryption methods to safeguard the confidentiality and integrity of the immersive content. Various encryption techniques are employed to protect VR streams [26], [24], [12], and these methods play a crucial role in preventing unauthorized access, data tampering, and eavesdropping. Common encryption standards such as Advanced Encryption Standard (AES) are often utilized to encrypt the 360 video data. AES is a symmetric encryption algorithm that ensures strong protection by using a secret key to encrypt and decrypt the data. In the context of VR streaming, this encryption method ensures that only authorized users with the appropriate decryption key can access and view the immersive content.

However, the choice of encryption strength in a cloud environment involves a trade-off between security and computational overhead. Increasing the encryption strength, such as moving from 128-bit to 256-bit keys in AES, enhances the security of the encrypted data but also requires more computational resources for encryption

and decryption processes. In a cloud environment where resources are shared among multiple users and applications, the computational overhead of stronger encryption can impact performance and increase latency. Striking the right balance is essential, considering factors such as the sensitivity of the VR content and the available computational resources. Cloud service providers often provide a range of encryption options, allowing users to tailor their security measures based on specific needs and performance considerations.

The trade-offs between encryption strength and computational overhead highlight the need for a nuanced approach in designing secure 360 VR video streaming solutions in the cloud. As technology advances, innovations in encryption algorithms and optimizations in cloud infrastructure will likely contribute to more efficient and secure methods, allowing for enhanced protection without compromising the overall performance of VR streaming experiences.

VII. AUTHENTICATION AND ACCESS CONTROL

In the landscape of secure 360 virtual reality (VR) video streaming in the cloud, robust authentication mechanisms are paramount to ensure that only authorized users have access to the immersive content. Authentication verifies the identity of users seeking entry to the VR streaming platform, preventing unauthorized access and safeguarding the sensitive nature of virtual experiences. Traditional username and password authentication may be augmented with multi-factor authentication (MFA), requiring users to provide additional verification factors such as biometric data or temporary codes sent to their mobile devices. MFA adds an extra layer of security, reducing the risk of unauthorized access even if login credentials are compromised. Biometric authentication methods, such as fingerprint or facial recognition, enhance the user experience while bolstering security in the cloud-based VR context.

In conjunction with robust authentication, access control policies and methods play a crucial role in managing and enforcing authorized access to 360 video streams. Access control policies define who can access what resources and under what conditions. Role-based access control (RBAC) is commonly employed, assigning specific roles to users based on their responsibilities and granting corresponding permissions. This ensures that users have access only to the functionalities and content necessary for their designated roles, limiting the potential for misuse or unauthorized viewing. Additionally, attribute-based access control (ABAC) considers various attributes, such as user attributes and environmental conditions, in making access decisions. Implementing these access control measures ensures a fine-grained and secure management of user privileges, contributing to the overall integrity of the 360 VR video streaming experience in the cloud.

VIII. CONTENT DELIVERY NETWORKS (CDNS) FOR VR

Content Delivery Networks (CDNs) play a crucial role in enhancing both the performance and security of 360 virtual reality (VR) video streaming in the cloud. CDNs are distributed networks of servers strategically placed around the globe to reduce latency and accelerate the delivery of content to end-users. In the context of 360 VR video streaming, CDNs help overcome bandwidth challenges and optimize the distribution of high-quality immersive content. By strategically caching and delivering VR video streams from servers closer to end-users, CDNs minimize the distance data must travel, reducing latency and ensuring a smoother, more immersive experience.

Security is another key aspect where CDNs contribute to the overall integrity of 360 VR video streaming. CDNs often employ security features such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption to protect data in transit. This ensures that the 360-degree video content is securely delivered from the cloud to the end-user device, preventing eavesdropping or tampering during transmission. Additionally, CDNs help mitigate Distributed Denial of Service (DDoS) attacks by distributing the load across multiple servers, making it more challenging for malicious actors to overwhelm a single point of entry.

To optimize CDNs for VR content delivery within a cloud infrastructure, several considerations come into play. First, the CDN must be geographically distributed to ensure that VR content is cached and delivered from servers located close to the end-users, reducing latency. Second, CDNs need to support adaptive streaming protocols, allowing for dynamic adjustments to the quality of the VR stream based on the viewer's network conditions. Furthermore, CDNs can benefit from edge computing capabilities, where certain processing tasks are offloaded to the edge servers, reducing the burden on the central cloud infrastructure and further minimizing latency for VR applications.

In conclusion, the strategic deployment and optimization of CDNs in a cloud environment significantly contribute to the success of secure 360 VR video streaming. By improving both performance and security, CDNs play a pivotal role in providing users with a seamless and immersive virtual reality experience.

IX. EXAMPLES

Suppose a virtual reality gaming platform seeks to deliver an immersive experience to users through secure 360 video streaming in the cloud. Leveraging cloud services such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform, the platform can implement robust security measures, including encryption, secure authentication, and access controls. The cloud infrastructure allows the platform to scale dynamically, adapting to varying user demands and ensuring low-latency streaming for a seamless VR gaming experience.

In this hypothetical case, the success of the implementation lies in the ability to balance security with performance. Utilizing a Content Delivery Network (CDN) in conjunction with cloud services helps optimize the delivery of 360 VR video streams, reducing latency and enhancing the overall user experience. Lessons learned from such implementations emphasize the importance of continuous monitoring, regular security audits, and staying abreast of emerging technologies to adapt and refine security measures as the virtual reality landscape evolves.

While specific case studies may vary, success in secure 360 VR video streaming implementations generally involves a holistic approach that addresses both the technical and user experience aspects. The ability to learn from challenges, iterate on solutions, and prioritize user security contributes to the ongoing refinement of secure VR content delivery in the cloud.

X. FUTURE TRENDS AND RESEARCH DIRECTIONS

The landscape of secure 360 virtual reality (VR) video streaming in the cloud is continually evolving, driven by emerging trends and technologies that enhance the overall immersive experience while addressing security concerns. One notable trend is the integration of blockchain technology for secure content distribution. Blockchain offers decentralized and tamper-resistant storage, ensuring the integrity of 360 VR video streams. By leveraging smart contracts, content creators can enforce secure licensing and monetization, providing a transparent and traceable framework for intellectual property protection.

Another emerging trend is the exploration of edge computing for optimized 360 VR video streaming. Edge computing involves processing data closer to the end-user device, reducing latency and improving real-time interactions in VR applications. By offloading certain processing tasks to edge servers, cloud providers can enhance the overall performance of VR content delivery. Additionally, machine learning [21] and artificial intelligence are being applied to optimize content delivery based on user preferences and network conditions, contributing to a more personalized and responsive VR streaming experience.

Looking ahead, potential areas for future research and development in secure 360 VR video streaming include advancements in immersive technologies such as augmented reality (AR) and extended reality (XR). Integrating AR elements into 360 VR video streams could lead to more interactive and dynamic experiences. Furthermore, researchers may explore the application of zero-trust security models in the context of VR, ensuring that trust is never assumed, and continuous authentication and authorization mechanisms are in place.

In the realm of content protection, watermarking techniques and digital rights management (DRM) for 360 VR content are areas that warrant further exploration. These technologies can enhance the security of intellectual property and prevent unauthorized distribution. Additionally, efforts to standardize security protocols specific to VR streaming and the development of industry-wide best practices will be essential to establish a robust security framework for the growing ecosystem of immersive content. As VR technology continues to evolve, the intersection of security and innovation will shape the future of secure 360 VR video streaming in the cloud.

The review paper on secure 360 virtual reality (VR) video streaming in the cloud provides a comprehensive exploration of the challenges, strategies, and innovations within this dynamic field. One key finding emphasizes the critical role of encryption in ensuring the security of 360 VR content. The paper underscores the importance of robust encryption methods, such as Advanced Encryption Standard (AES), to safeguard data integrity and confidentiality during content delivery. It further delves into the nuanced balance between encryption strength and computational overhead, highlighting the trade-offs involved in choosing the appropriate encryption protocols for cloud-based VR applications.

Another significant insight revolves around the pivotal role of authentication mechanisms and access control policies in securing user access to VR content in the cloud. The review paper illuminates how multi-factor authentication and role-based access control contribute to a secure streaming environment, preventing unauthorized access and protecting sensitive virtual experiences. It explores real-world examples and hypothetical case studies, demonstrating the practical implementation of these security measures in cloud-based VR systems.

Furthermore, the review paper delves into emerging trends and technologies shaping the landscape of

secure 360 VR video streaming. It discusses the integration of blockchain for decentralized and tamper-resistant content distribution, as well as the exploration of edge computing to optimize performance and reduce latency. The insights provided in the review paper serve as a valuable resource for researchers, practitioners, and industry stakeholders, offering a roadmap for navigating the complex intersection of security, technology, and user experience in the realm of 360 VR video streaming in the cloud.

XI. CONCLUSION

The widespread adoption of 360 virtual reality (VR) video streaming hinges on effectively addressing security concerns inherent to this immersive content delivery. Security is a paramount consideration due to the unique and often sensitive nature of VR experiences. As users engage with 360 VR content, the need to safeguard data integrity, ensure confidentiality, and protect against unauthorized access becomes crucial. Privacy concerns are heightened in VR, where users may share personal spaces or engage in educational and training simulations. Therefore, a robust security framework is imperative to establish trust among users and stakeholders.

Emphasizing security in 360 video streaming is essential for building confidence in the technology and encouraging broader adoption. Without adequate security measures, users may be hesitant to engage with VR content, fearing potential breaches or unauthorized access to their virtual experiences. Moreover, as VR applications expand into various sectors such as healthcare, education, and enterprise, the protection of sensitive data and intellectual property becomes paramount. Addressing security concerns not only safeguards user privacy but also fosters a conducive environment for the development of diverse and innovative VR applications, contributing to the overall growth and acceptance of this transformative technology.

In practical terms, implementing encryption protocols, secure authentication mechanisms, and access controls are fundamental steps toward ensuring the security of 360 VR video streaming in the cloud. By proactively addressing security concerns, the VR industry can build a foundation of trust, enabling users to fully embrace the immersive potential of 360 VR experiences and fostering the broader adoption of virtual reality across various domains.

REFERENCES

[1] Alam A. Cloud-based e-learning: scaffolding the environment for adaptive e-learning ecosystem based on cloud computing infrastructure. InComputer Communication, Networking and IoT: Proceedings of 5th ICICC 2021, Volume 2 2022 Oct 5 (pp. 1-9). Singapore: Springer Nature Singapore.

[2] Alouffi B, Hasnain M, Alharbi A, Alosaimi W, Alyami H, Ayaz M. A systematic literature review on cloud computing security: threats and mitigation strategies. IEEE Access. 2021 Apr 14;9:57792-807.

[3] 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.

[4] Blum N, Lachapelle S, Alvestrand H. WebRTC: Real-time communication for the open web platform. Communications of the ACM. 2021 Jul 26;64(8):50-4.

[5] Burdinat C, Raulet M, Toullec E. Encoding and Storing Only Once: The Road to CMAF Adoption. SMPTE Motion Imaging Journal. 2023 Jul 27;132(7):39-44.

[6] Fan CL, Yen SC, Huang CY, Hsu CH. Optimizing fixation prediction using recurrent neural networks for 360$^{\circ} $ video streaming in head-mounted virtual reality. IEEE Transactions on Multimedia. 2019 Jul 29;22(3):744-59.

[7] Fei Z, Wang F, Wang J, Xie X. QoE evaluation methods for 360-degree VR video transmission. IEEE Journal of Selected Topics in Signal Processing. 2019 Nov 28;14(1):78-88.

[8] Gül S, Podborski D, Son J, Bhullar GS, Buchholz T, Schierl T, Hellge C. Cloud rendering-based volumetric video streaming system for mixed reality services. InProceedings of the 11th ACM multimedia systems conference 2020 May 27 (pp. 357-360).

[9] Hooft JV, Vega MT, Petrangeli S, Wauters T, Turck FD. Tile-based adaptive streaming for virtual reality video. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM). 2019 Dec 16;15(4):1-24.

[10] Hu M, Luo X, Chen J, Lee YC, Zhou Y, Wu D. Virtual reality: A survey of enabling technologies and its applications in IoT. Journal of Network and Computer Applications. 2021 Mar 15;178:102970.

[11] Huang X, Riddell J, Xiao R. Virtual Reality Telepresence: 360-Degree Video Streaming with Edge-Compute Assisted Static Foveated Compression. IEEE Transactions on Visualization and Computer Graphics. 2023 Oct 3.

[12] Islam MT, Rothenberg CE, Gomes PH. Predicting XR Services QoE with ML: Insights from In-band Encrypted QoS Features in 360-VR. In2023 IEEE 9th International Conference on Network Softwarization (NetSoft) 2023 Jun 19 (pp. 80-88). IEEE.

[13] Jeong JB, Lee S, Ryu IW, Le TT, Ryu ES. Towards viewport-dependent 6DoF 360 video tiled streaming for virtual reality systems. InProceedings of the 28th ACM International Conference on Multimedia 2020 Oct 12 (pp. 3687-3695).

[14] Kazarian A, Teslyuk V. Development of a Virtual Cloud-Based Traffic Rules Learning Simulator Using Spherical Video Streams. In2023 IEEE 13th International Conference on Electronics and Information Technologies (ELIT) 2023 Sep 26 (pp. 181-185). IEEE.

[15] 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.

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

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

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

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

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

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

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

[23] Tang Z, Feng X, Xie Y, Phan H, Guo T, Yuan B, Wei S. Vvsec: Securing volumetric video streaming via benign use of adversarial perturbation. InProceedings of the 28th ACM International Conference on Multimedia 2020 Oct 12 (pp. 3614-3623).

[24] Tang Z, Feng X, Xie Y, Phan H, Guo T, Yuan B, Wei S. Vvsec: Securing volumetric video streaming via benign use of adversarial perturbation. InProceedings of the 28th ACM International Conference on Multimedia 2020 Oct 12 (pp. 3614-3623).

[25] Teng L, Zhai G, Wu Y, Min X, Zhang W, Ding Z, Xiao C. QoE driven VR 360° video massive MIMO transmission. IEEE Transactions on Wireless Communications. 2021 Jul 9;21(1):18-33.

[26] Thanh Le T, Jeong J, Ryu ES. Efficient transcoding and encryption for live 360 CCTV system. Applied Sciences. 2019 Feb 21;9(4):760.

[27] Vinoth S, Vemula HL, Haralayya B, Mamgain P, Hasan MF, Naved M. Application of cloud computing in banking and e-commerce and related security threats. Materials Today: Proceedings. 2022 Jan 1;51:2172-5.

[28] Wohlgenannt I, Simons A, Stieglitz S. Virtual reality. Business & Information Systems Engineering. 2020 Oct;62:455-61.

[29] Xiong J, Hsiang EL, He Z, Zhan T, Wu ST. Augmented reality and virtual reality displays: emerging technologies and future perspectives. Light: Science & Applications. 2021 Oct 25;10(1):216.

[30] Yaqoob A, Bi T, Muntean GM. A survey on adaptive 360 video streaming: Solutions, challenges and opportunities. IEEE Communications Surveys & Tutorials. 2020 Jul 3;22(4):2801-38.

[31] Zhang R, Liu J, Liu F, Huang T, Tang Q, Wang S, Yu FR. Buffer-aware virtual reality video streaming with personalized and private viewport prediction. IEEE Journal on Selected Areas in Communications. 2021 Oct 11;40(2):694-709.

[32] Zheng M, Tie Y, Zhu F, Qi L, Gao Y. Research on panoramic stereo live streaming based on the virtual reality. In2021 IEEE International Symposium on Circuits and Systems (ISCAS) 2021 May 22 (pp. 1-5). IEEE.

[33] 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.

