International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Securing Immersive Realms: A Review of Security Measures in 360-Degree Virtual Reality Video Streaming

Koffka Khan

Lecturer in the Department of Computing and Information Technology, The University of the West Indies, St Augustine, Trinidad and Tobago

Abstract: ***This review paper explores the multifaceted landscape of security challenges and solutions in the realm of 360-degree Virtual Reality (VR) video streaming. As the popularity of immersive VR experiences grows, so does the need to address vulnerabilities unique to this domain. The paper systematically surveys existing literature, analyzing the spectrum of security threats, ranging from data integrity and privacy concerns to potential malicious attacks on VR streaming platforms. It delves into the intricacies of securing 360-degree VR video content, discussing encryption methods, watermarking techniques, and authentication protocols designed to protect against unauthorized access and content manipulation. Furthermore, the review critically assesses the performance of various security mechanisms in the context of real-time streaming, considering factors such as latency and bandwidth constraints. Emerging technologies, such as blockchain and artificial intelligence, are also evaluated for their potential contributions to enhancing the security posture of 360-degree VR video streaming. The paper concludes by outlining future research directions and emphasizing the importance of a comprehensive and adaptive security framework to ensure the integrity and privacy of users engaging in immersive VR experiences.***

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

1. Introduction

In recent years, there has been a significant surge in the popularity of 360-degree virtual reality (VR) video streaming[1], [5], [20], [18], [3], which is a variant of adaptive video streaming [7], [8], [9], [10], [11], [12]. This immersive technology allows users to experience content in a more engaging and lifelike manner, providing a sense of presence and interaction with the virtual environment. The growth of VR headsets and the increasing accessibility of high-quality 360-degree cameras have contributed to the widespread adoption of this technology. Some features are:

- Enhanced User Experience: 360-degree VR video streaming offers a more immersive and interactive experience compared to traditional video formats. Users can explore the virtual environment by moving their heads or using controllers, creating a sense of presence that goes beyond conventional video watching.
- Diverse Content Creation: The popularity of 360-degree VR video is not limited to a specific industry. It has found applications in various fields such as entertainment, gaming, education, tourism, and real estate. From virtual tours and live events to cinematic experiences, content creators are exploring diverse ways to leverage this technology.
- Advancements in VR Technology: Ongoing advancements in VR hardware, including more affordable and user-friendly VR headsets, have contributed to the increased adoption of 360-degree VR video streaming. This has made the technology more accessible to a broader audience, fostering its integration into mainstream media.
- Growing Social VR Platforms: Social VR platforms and virtual spaces have gained popularity, enabling users to share and consume 360-degree content together. This social aspect enhances the overall appeal of VR streaming, as users can virtually connect with others and experience content collaboratively.

While the growth of 360-degree VR video streaming brings about exciting possibilities, it also introduces unique security challenges that must be addressed to ensure a safe and reliable user experience. Some of these are:

- Privacy Concerns: VR environments often involve user interaction within a virtual space. This raises concerns about user privacy, as personal data and interactions may be at risk. Implementing robust privacy measures is crucial to protect users from potential breaches and unauthorized access.
- Content Piracy: With the increasing popularity of VR content, the risk of unauthorized distribution and piracy rises. Protecting intellectual property and ensuring that content creators receive proper compensation becomes a priority, necessitating effective digital rights management (DRM) solutions.
- Cybersecurity Threats: As with any online platform, VR streaming services are susceptible to cybersecurity threats such as hacking, data breaches, and distributed denial-of-service (DDoS) attacks. Implementing robust security protocols, encryption, and regular cybersecurity audits is essential to safeguard both user data and the integrity of the VR experience.
- Identity and Authentication Challenges: Verifying user identity in VR environments poses unique challenges. Ensuring secure authentication processes is crucial to prevent unauthorized access and protect user accounts from being compromised.

In conclusion, the increasing popularity of 360-degree VR video streaming presents exciting opportunities across various industries. However, addressing the security challenges associated with this technology is paramount to foster trust among users and facilitate its continued growth in a secure and sustainable manner.

2. Security Threats in 360-Degree VR Video Streaming

Here are Security Threats Inherent to 360-Degree VR Video Streaming[19], [14], [15], [16]:

- Data Integrity Risks: Tampering and Manipulation: Malicious actors may attempt to alter or manipulate the 360-degree VR content during streaming, leading to a distorted or false representation of the virtual environment.
- Corruption during Transmission: Issues such as packet loss or interference during data transmission can result in corrupted VR content, affecting the overall user experience and potentially introducing security vulnerabilities.
- Privacy Breaches: Location Tracking and Surveillance: VR systems may collect location data and user interactions within the virtual environment. Unauthorized access to this information could lead to privacy breaches and tracking of users' movements and activities.
- User Data Harvesting: Personal information stored within VR platforms, such as user profiles and preferences, may be targeted for unauthorized data harvesting, leading to potential privacy violations.
- Unauthorized Access: Account Hijacking: Weak authentication mechanisms may make user accounts susceptible to hijacking. Unauthorized access can lead to the theft of personal information, unauthorized use of paid content, or even disruption of the user's VR experience.
- Content Piracy: VR content is at risk of being illegally copied and distributed, undermining the intellectual property rights of content creators and potentially causing financial losses.

Here are Network-Related Threats:

- Man-in-the-Middle (MitM) Attacks: Attackers may intercept and alter the communication between the VR device and the streaming server. This can result in unauthorized access to sensitive information or manipulation of the VR content in real-time.
- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks: VR streaming services may be targeted with attacks that overload the network infrastructure, causing disruptions in service availability and potentially compromising the overall VR experience.
- Device Security Risks: VR Headset Vulnerabilities: Security vulnerabilities in VR headset software or firmware can be exploited by attackers to gain control of the device, potentially leading to unauthorized access to user data and compromising the integrity of the VR experience.
- Peripheral Device Exploitation: Malicious actors may target peripheral devices connected to VR systems, such as controllers or sensors, to compromise the overall security of the VR setup.
- Social Engineering Attacks:
- Phishing and Deceptive Practices: Users may be tricked into providing sensitive information or login credentials through phishing attempts conducted within the VR environment, exploiting the immersive nature of the platform.

Addressing these security threats requires a comprehensive approach, including the implementation of robust encryption, authentication mechanisms, secure coding practices, regular software updates, and user education to promote awareness and responsible use of VR platforms. As the popularity of 360-degree VR video streaming continues to grow, the industry must remain vigilant in mitigating these evolving security risks.

3. Security Mechanisms for 360-Degree VR Video Content

Here are Encryption Techniques for Securing 360-Degree VR Video Content [6], [17], [13]:

1) End-to-End Encryption:

- Description: End-to-end encryption ensures that the content is encrypted on the sender's side, transmitted in an encrypted form, and only decrypted on the recipient's end. This prevents unauthorized access or tampering during the transmission of 360-degree VR video content.
- Implementation: Industry-standard encryption protocols such as TLS (Transport Layer Security) can be employed to establish secure communication channels between VR streaming servers and client devices.

2) Homomorphic Encryption:

- Description: Homomorphic encryption allows computations to be performed on encrypted data without the need for decryption. This can be beneficial for processing and rendering encrypted 360-degree VR video content on the client side without exposing the raw data.
- Implementation: While homomorphic encryption is computationally intensive, advancements in this field may offer more practical solutions for securing VR content in the future.

3) Content Encryption Key Rotation:

- Description: Regularly changing the encryption keys used to protect the VR content adds an extra layer of security. Even if a key is compromised, it limits the exposure of the entire content.
- Implementation: Implementing key rotation protocols to periodically update and rotate encryption keys used for protecting 360-degree VR video streams.

4) Here are Watermarking Methods to Deter Unauthorized Distribution and Manipulation:

a) Visible Watermarking:

- Description: Embedding visible marks or logos directly into the VR content to discourage unauthorized distribution. While it does not prevent manipulation, it acts as a deterrent.
- Implementation: Adding a visible watermark during post-production or as part of the streaming process to identify the content's source.

b) Invisible Watermarking (Digital Watermarking):

- Description: Embedding imperceptible marks within the VR content that can be detected using specialized

algorithms. This aids in tracking and identifying the source of unauthorized distribution.
- Implementation: Utilizing digital watermarking techniques to insert invisible marks that survive compression and other transformations.

c) **Fingerprinting:**
- Description: Creating a unique identifier or fingerprint for each instance of VR content. This can be used to trace the origin of unauthorized copies.
- Implementation: Applying fingerprinting algorithms to generate unique identifiers for 360-degree VR videos, enabling tracking and identification.

Here are Authentication Protocols and Access Controls for VR Streaming Platforms:

a) **Two-Factor Authentication (2FA):**
- Description: Adding an extra layer of security by requiring users to provide two forms of identification before accessing their accounts or VR content.
- Implementation: Implementing 2FA mechanisms such as SMS codes, authentication apps, or biometric authentication for VR streaming platform logins.

b) **Secure Tokenization:**
- Description: Instead of transmitting sensitive information like user credentials directly, tokens are used as temporary access credentials. These tokens are difficult to intercept and provide a secure means of authentication.
- Implementation: Employing secure tokenization protocols to authenticate and authorize users without exposing sensitive information during the VR streaming session.

c) **Role-Based Access Control (RBAC):**
- Description: Implementing RBAC allows administrators to define roles and permissions for different user types. This ensures that only authorized users have access to specific VR content or features.
- Implementation: Assigning roles to users based on their responsibilities and implementing access controls accordingly within the VR streaming platform.

Implementing a combination of these encryption, watermarking, authentication, and access control methods can significantly enhance the security of 360-degree VR video content and the overall streaming platform. As technology evolves, staying updated with the latest security practices and adopting robust measures is essential to protect against emerging threats.

4. Performance Considerations in Real-Time Streaming

Here are some Impact of Security Mechanisms on Real-Time Streaming Performance of 360-Degree VR Content [4]:

a) **Latency:**
- Security Mechanisms: Encryption, particularly strong end-to-end encryption, can introduce additional processing overhead, potentially leading to increased latency in real-time streaming. Complex encryption algorithms or frequent key rotations may contribute to delays.
- Impact on Performance: Higher latency can result in delayed response times to user interactions, affecting the overall immersive experience in 360-degree VR content. Balancing strong encryption with minimal latency is crucial for maintaining real-time interactivity.

b) **Bandwidth Requirements:**
- Security Mechanisms: Encrypted data tends to be larger in size than unencrypted data, leading to increased bandwidth requirements. This is especially relevant in VR streaming, where high-quality, high-resolution 360-degree videos are transmitted.
- Impact on Performance: Higher bandwidth requirements can strain network resources, causing potential buffering issues and reducing the quality of the VR stream. Optimizing encryption algorithms and employing compression techniques can help mitigate these challenges.

c) **User Experience:**
- Security Mechanisms: While robust security mechanisms are essential for protecting 360-degree VR content, overly complex or intrusive security measures can impact the overall user experience. This includes authentication processes, access controls, and any visible or invisible watermarks.
- Impact on Performance: Cumbersome security procedures may lead to user frustration, longer onboarding times, or a less seamless transition into the VR experience. Striking a balance between security and a smooth user experience is critical.

d) **Hardware and Software Compatibility:**
- Security Mechanisms: The choice of encryption algorithms and security protocols can impact compatibility with VR hardware and software. Some encryption methods may require more processing power or specific software support.
- Impact on Performance: Incompatible security mechanisms can result in degraded performance, system crashes, or failure to render VR content properly. Ensuring alignment with industry standards and compatibility testing is vital for a seamless experience.

e) **Dynamic Content Adaptation:**
- Security Mechanisms: Adaptive streaming technologies, which dynamically adjust the quality of the VR content based on network conditions, may need to account for the additional processing overhead introduced by security mechanisms.
- Impact on Performance: Security implementations should not hinder the adaptive streaming's ability to optimize the content quality based on the user's network connection. Adaptive streaming may need to dynamically adjust based on the resource demands of encryption and other security features.

f) Network Stability and Reliability:

- Security Mechanisms: The introduction of security measures can exacerbate the impact of network instability, leading to potential disruptions in the streaming experience.
- Impact on Performance: In scenarios where network conditions are less than optimal, robust security measures should be implemented without compromising the stability and reliability of the VR stream. Error correction mechanisms and adaptive protocols can be crucial in maintaining a smooth experience.

g) Optimizing Security Measures for Real-Time Streaming:

- Efficient Encryption Algorithms: Choose encryption algorithms that strike a balance between security and efficiency. Some algorithms are designed to minimize computational overhead while maintaining strong security.
- Compression Techniques: Implement compression techniques to reduce the size of encrypted data, helping to mitigate the impact on bandwidth requirements.
- Caching and Content Delivery Networks (CDNs): Utilize caching mechanisms and CDNs to optimize content delivery, reducing latency and improving the overall streaming performance.
- Continuous Testing and Optimization: Regularly test the performance impact of security mechanisms and make optimizations based on advancements in encryption technology and streaming protocols.

Balancing robust security measures with optimal real-time streaming performance is a continuous challenge, requiring a thorough understanding of the specific requirements and constraints of 360-degree VR content delivery. As technology evolves, ongoing research and development efforts are essential to refine security implementations and enhance the overall user experience.

5. Emerging Technologies for Enhanced Security

How Blockchain[2] in used to Bolster Security of 360-Degree VR Video Streaming:

a) Content Authentication and Integrity:
Role: Blockchain can be used to create a decentralized and tamper-proof ledger to verify the authenticity and integrity of 360-degree VR content. Each piece of content can be uniquely identified and timestamped, ensuring that it has not been altered or tampered with during distribution.

b) Digital Rights Management (DRM):
Role: Blockchain can enhance DRM by providing a secure and transparent way to manage digital rights. Smart contracts on the blockchain can enforce access controls, ensuring that only authorized users can view or distribute VR content. This helps prevent unauthorized access and piracy.

c) Smart Contracts for Royalties and Licensing:
Role: Blockchain-based smart contracts can automate royalty payments and licensing agreements for content creators in real-time. This ensures fair compensation for VR content creators and minimizes disputes, fostering a more transparent and equitable ecosystem.

d) Decentralized Content Distribution:
Role: Blockchain enables decentralized content distribution networks, reducing reliance on centralized servers. This can enhance the robustness and security of 360-degree VR streaming by distributing content across a network of nodes, making it more resistant to DDoS attacks and improving scalability.

e) Tokenization of VR Assets:
Role: Blockchain can facilitate the tokenization of virtual assets within the VR environment. This includes virtual real estate, items, or experiences. Blockchain-based tokens can be securely managed and traded, enhancing the security of virtual economies within VR platforms.

Here is how Artificial Intelligence (AI) is used to Bolster Security of 360-Degree VR Video Streaming:

Behavioral Analysis for User Authentication:
Role: AI-powered behavioral analysis can be used to strengthen user authentication in VR streaming platforms. By analyzing user behavior, such as hand movements or interaction patterns, AI systems can detect anomalies and identify potential unauthorized access.

Anomaly Detection in VR Environments:
Role: AI algorithms can continuously analyze user interactions and content consumption patterns to detect anomalies that may indicate security threats. This includes identifying unusual navigation or viewing behaviors that may signal a potential security breach.

Dynamic Threat Detection and Response:
Role: AI can dynamically adapt security measures based on evolving threats. Machine learning models can analyze streaming patterns in real-time, identifying potential threats and triggering adaptive security responses to protect against unauthorized access or content manipulation.

Predictive Analytics for Content Distribution:
Role: AI-driven predictive analytics can optimize content distribution by anticipating peak demand times, ensuring that VR streaming platforms can handle increased traffic securely. This helps prevent performance issues and ensures a consistent user experience.

Automated Content Moderation:
Role: AI can be employed for automated content moderation within VR environments, identifying and filtering out inappropriate or malicious content. This ensures a safer and more secure virtual space for users.

Machine Learning for Network Security:
Role: AI-driven machine learning algorithms can enhance network security by identifying and mitigating potential threats, such as DDoS attacks or unauthorized access

attempts. These systems can adapt and learn from patterns, providing a proactive defense against emerging threats.

We now discuss the Integration of Blockchain and AI:

- Secure Identity Management: Combining blockchain and AI can enhance secure identity management within VR platforms, ensuring that user identities are securely stored on a tamper-proof blockchain and leveraging AI for continuous authentication.
- AI-Enhanced Smart Contracts: AI algorithms can be integrated into smart contracts on the blockchain to create more sophisticated and adaptive contract terms. For example, AI can dynamically adjust access controls based on user behavior or threat detection.
- Blockchain-based AI Training Data Security: Blockchain can be used to secure the training data used by AI models, ensuring the integrity and authenticity of the data. This is particularly important for AI systems that analyze user behavior in VR environments.

In conclusion, the integration of emerging technologies like blockchain and artificial intelligence holds great potential for enhancing the security of 360-degree VR video streaming. These technologies provide innovative solutions to address challenges related to content authentication, access control, behavioral analysis, and overall platform security. As the VR industry continues to evolve, leveraging the synergies between blockchain and AI can contribute to a more secure and robust virtual reality experience.

6. Challenges and Future Directions

Here are Current Challenges and Limitations in Securing 360-Degree VR Video Streaming:

High Computational Overhead:
Challenge: Strong encryption and security measures can introduce significant computational overhead, leading to increased latency and potentially degrading the real-time streaming performance of 360-degree VR content.

Complexity of Authentication in VR Environments:
Challenge: Designing effective and user-friendly authentication methods in VR environments can be challenging. Balancing security with a seamless user experience is crucial, as traditional authentication approaches may not translate well into the immersive VR space.

Privacy Concerns and User Data Handling:
Challenge: VR platforms often collect sensitive user data for personalization and interaction tracking. Balancing the need for data-driven experiences with user privacy is a complex challenge, especially as VR systems expand their capabilities.

Content Piracy and Digital Rights Management:
Challenge: Despite advancements in DRM technologies, content piracy remains a significant concern. Protecting intellectual property and ensuring fair compensation for content creators in the context of 360-degree VR video streaming pose ongoing challenges.

Standardization and Interoperability:
Challenge: Lack of standardized security protocols and interoperability standards across VR platforms can hinder the development of consistent and universally applicable security measures. This fragmentation can create vulnerabilities and complicate security implementations.

Emerging Threats and Evolving Attack Vectors:
Challenge: As 360-degree VR video streaming gains popularity, new and sophisticated security threats are likely to emerge. Predicting and addressing these evolving threats requires continuous research and proactive security measures.

Integration of Blockchain and AI:
Limitation: While promising, the integration of blockchain and AI introduces challenges related to scalability, interoperability, and the development of standardized approaches for effective collaboration between these technologies in the context of VR security.

Here are Potential Avenues for Future Research and Development:

Optimized Encryption and Compression Techniques:
Research Focus: Develop more efficient encryption and compression techniques tailored for 360-degree VR video streaming. This includes exploring lightweight encryption algorithms and compression methods that minimize computational overhead without compromising security.

Biometric Authentication in VR Environments:
Research Focus: Investigate the feasibility and security of implementing biometric authentication methods in VR, such as facial recognition or hand gesture recognition. Designing secure and user-friendly biometric authentication for VR is a promising avenue for research.

Privacy-Preserving VR Interaction Tracking:
Research Focus: Explore privacy-preserving methods for VR interaction tracking. This involves developing techniques that allow for personalized experiences without compromising user privacy, potentially leveraging cryptographic protocols and decentralized technologies.

Blockchain-Based Digital Rights Management:
Research Focus: Further research blockchain-based solutions for digital rights management in VR. This includes exploring smart contract implementations that enhance the transparency, efficiency, and security of licensing and royalty agreements in the VR content ecosystem.

Standardization Efforts for VR Security:
Research Focus: Contribute to the development of standardized security protocols and interoperability standards for VR platforms. Collaborative efforts among industry stakeholders can lead to more secure and consistent implementations across different VR ecosystems.

Behavioral Analysis and AI-Driven Threat Detection:
Research Focus: Advance AI-driven behavioral analysis for threat detection in VR environments. Research can focus on

developing machine learning models that adapt to evolving threats and identify anomalous behavior patterns indicative of security risks.

Human Factors in VR Security:
Research Focus: Investigate the human factors involved in VR security, including user perceptions of security measures, the impact of security on user experience, and the effectiveness of security awareness training within VR environments.

Quantum-Safe Encryption for VR:
Research Focus: Anticipate future security challenges by exploring quantum-safe encryption methods for 360-degree VR video streaming. Research in post-quantum cryptography can help future-proof VR security against the potential threat of quantum computers.

User-Centric Security Design:
Research Focus: Adopt a user-centric approach to security design in VR. Research can focus on understanding user expectations, preferences, and behaviors related to security, leading to the development of more user-friendly and effective security measures.

Cross-Disciplinary Collaboration:
Research Focus: Foster cross-disciplinary collaboration between VR experts, cybersecurity researchers, and privacy advocates. A holistic approach that considers technical, human, and ethical aspects is essential for addressing the multifaceted challenges in securing 360-degree VR video streaming.

As the field of 360-degree VR video streaming continues to evolve, addressing these challenges and pursuing innovative research directions will contribute to the development of more secure, reliable, and user-friendly VR experiences. Collaboration among researchers, industry stakeholders, and policymakers will play a crucial role in shaping the future of VR security.

7. Conclusion

Here is a Summary of Key Findings and Insights:

- Popularity of 360-Degree VR Video Streaming: The popularity of 360-degree VR video streaming has grown significantly, driven by advancements in VR technology, increased accessibility of VR devices, and diverse applications across industries.
- Security Challenges in 360-Degree VR: Securing 360-degree VR video streaming involves addressing challenges such as high computational overhead, complex authentication in VR environments, privacy concerns, content piracy, emerging threats, and the need for standardization.
- Contributions of Emerging Technologies: Blockchain and artificial intelligence (AI) show promise in bolstering the security of 360-degree VR video streaming. Blockchain can enhance content authentication, DRM, and decentralized content distribution, while AI can strengthen user authentication, anomaly detection, and predictive analytics.
- Impact on Real-Time Streaming Performance: Security mechanisms, including encryption and watermarking, can impact real-time streaming performance by introducing latency, increasing bandwidth requirements, and influencing the overall user experience. Balancing strong security with optimal performance is crucial.
- Optimization Strategies: Optimization strategies, such as efficient encryption algorithms, compression techniques, and the integration of blockchain and AI, are essential for mitigating the performance impact of security measures in 360-degree VR video streaming.
- Future Research Avenues: Future research should focus on optimized encryption and compression techniques, biometric authentication in VR, privacy-preserving interaction tracking, blockchain-based DRM, standardization efforts, AI-driven threat detection, human factors in VR security, quantum-safe encryption, and user-centric security design.
- Comprehensive and Adaptive Security Framework: Emphasizing the importance of a comprehensive and adaptive security framework is crucial for the continued growth of 360-degree VR video streaming. This framework should address evolving threats, consider user-centric design, and leverage emerging technologies to create a secure and immersive VR experience.

In conclusion the dynamic landscape of 360-degree VR video streaming demands a security approach that is not only robust but also adaptive to the evolving challenges and user expectations. Balancing security with real-time streaming performance, user experience, and privacy considerations requires continuous research, innovation, and collaboration across disciplines. As the industry continues to mature, a comprehensive security framework that incorporates the latest advancements in encryption, blockchain, and AI will play a pivotal role in fostering trust, protecting content, and ensuring the sustainable growth of 360-degree VR video streaming.

References

[1] Anwar MS, Wang J, Ullah A, Khan W, Ahmad S, Fei Z. Measuring quality of experience for 360-degree videos in virtual reality. Science China Information Sciences. 2020 Oct;63:1-5.

[2] Bhattacharya P, Saraswat D, Dave A, Acharya M, Tanwar S, Sharma G, Davidson IE. Coalition of 6G and blockchain in AR/VR space: Challenges and future directions. IEEE Access. 2021 Dec 20;9:168455-84.

[3] Chiariotti F. A survey on 360-degree video: Coding, quality of experience and streaming. Computer Communications. 2021 Sep 1;177:133-55.

[4] Eltobgy O, Arafa O, Hefeeda M. Mobile streaming of live 360-degree videos. IEEE Transactions on Multimedia. 2020 Feb 14;22(12):3139-52.

[5] 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.

[6] Kattadige C, Raman A, Thilakarathna K, Lutu A, Perino D. 360NorVic: 360-degree video classification

from mobile encrypted video traffic. In Proceedings of the 31st ACM Workshop on Network and Operating Systems Support for Digital Audio and Video 2021 Jul 16 (pp. 58-65).

[7] Khan K, Goodridge W. B-DASH: broadcast-based dynamic adaptive streaming over HTTP. International Journal of Autonomous and Adaptive Communications Systems. 2019;12(1):50-74.

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

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

[10] 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.

[11] Khan K, Goodridge W. Rate oscillation breaks in HTTP on-off distributions: a DASH framework. International Journal of Autonomous and Adaptive Communications Systems. 2020;13(3):273-96.

[12] Khan K. A Framework for Meta-Learning in Dynamic Adaptive Streaming over HTTP. International Journal of Computing. 2023 Apr;12(2).

[13] Khan K. A Taxonomy for the Use of Quantum Computing in Drone Video Streaming Technology, International Journal of Innovative Science and Research Technology (IJISRT) 2023 (pp.2670-2681).

[14] Liu Y, Liu J, Argyriou A, Ma S, Wang L, Xu Z. 360-degree VR video watermarking based on spherical wavelet transform. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM). 2021 Apr 16;17(1):1-23.

[15] Miller MR, Herrera F, Jun H, Landay JA, Bailenson JN. Personal identifiability of user tracking data during observation of 360-degree VR video. Scientific Reports. 2020 Oct 15;10(1):17404.

[16] Ruan J, Xie D. Networked vr: State of the art, solutions, and challenges. Electronics. 2021 Jan 13;10(2):166.

[17] 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).

[18] Wei W, Han J, Xing Y, Xue K, Liu J, Zhuang R. MP-VR: An MPTCP-based adaptive streaming framework for 360-degree virtual reality videos. InICC 2021-IEEE International Conference on Communications 2021 Jun 14 (pp. 1-6). IEEE.

[19] 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.

[20] Zhang H, Yang Z, Mohapatra P. Wireless access to ultimate virtual reality 360-degree video. InProceedings of the International Conference on Internet of Things Design and Implementation 2019 Apr 15 (pp. 271-272).

Author Profile

Koffka Khan received the B.Sc., M.Sc., M.Phil. and D.Phil. degrees from the University of the West Indies, St. Augustine, Trinidad and Tobago. He is currently working as a Lecturer in the Department of Computing and Information Technology. He has to date published over 230 books and papers of international repute. His research interest includes multimedia communications, computational intelligence, routing protocols, wireless communications, and cryptography.