International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Comprehensive Review on Secure Video Streaming in Cloud Environments

Koffka Khan

Lecturer in Computer Science, Department of Information and Computer Technology, University of the West Indies, St. Augustine, Trinidad and Tobago

Abstract
The proliferation of cloud-based video streaming services has revolutionized the way users access and share multimedia content. However, the inherent security challenges associated with transmitting, storing, and delivering video data in cloud environments demand comprehensive solutions. This review paper aims to provide a thorough analysis of the state-of-the-art techniques and methodologies employed in ensuring secure video streaming in the cloud. It encompasses various aspects such as encryption, authentication, access control, and integrity verification to safeguard video content throughout its lifecycle.

Keywords: cloud, video streaming, services, multimedia, secure, encryption, integrity

1. Introduction

The advent of cloud computing has revolutionized the way digital content, especially videos, is delivered and consumed. Video streaming [7, 8, 9, 10] services in cloud environments have become integral to modern entertainment, communication, and education. With the ability to provide on-demand access to a vast array of video content, cloud-based video streaming has gained immense popularity, offering convenience and flexibility to users worldwide. This shift from traditional broadcasting methods to cloud-based streaming has led to a paradigm shift in the media and entertainment industry.

Cloud-based video streaming [14, 19, 2, 3] services leverage the scalability and accessibility of cloud infrastructure, allowing users to enjoy high-quality video content across various devices and locations. This evolution has not only transformed user experiences but has also presented new challenges related to the security of video content, user data, and the overall integrity of streaming services.

The motivation behind securing cloud-based video streaming services stems from the growing threat landscape in cybersecurity. As video streaming [11, 12, 13] platforms continue to expand their user base and content libraries, they become lucrative targets for malicious actors. Cybersecurity threats, including unauthorized access, data breaches, content piracy, and privacy violations, pose significant risks to both content providers and users.

The increasing sophistication of cyberattacks emphasizes the critical need for robust security measures to protect sensitive video content, user information, and the overall integrity of streaming platforms. The motivation for this review is to explore the security challenges faced by cloud-based video streaming services and examine the technologies and strategies employed to mitigate these risks, ensuring a secure and trustworthy streaming experience for users.

The scope of this review encompasses various aspects of securing video streaming in cloud environments [16, 1]. Key focus areas include:

Encryption: Examining encryption techniques employed to safeguard the confidentiality and integrity of video content during transmission and storage.

Authentication Mechanisms: Analyzing methods of user and device authentication to control access to video streaming services securely.

Access Control Models: Exploring role-based and attribute-based access control models for regulating user access to video content.

Integrity Verification: Assessing technologies such as digital signatures and blockchain for ensuring the integrity of video content in cloud-based streaming services.

By delving into these key areas, this review aims to provide insights into the current state of security measures employed by cloud-based video streaming services and identify future directions for research and development in this dynamic and rapidly evolving field.

The introduction sets the stage by presenting the escalating importance of video streaming in cloud environments, emphasizing its growing prevalence and impact. Motivation follows, underscoring the critical need for secure video streaming amidst the rising tide of cybersecurity threats. The scope of the review is then delineated, encompassing crucial aspects like encryption, authentication, access control, and integrity verification. Moving into the core of the paper, the section on security challenges in cloud video streaming explores unauthorized access risks, potential threats to data integrity, and privacy concerns associated with user data in cloud-based streaming services. The subsequent sections delve into specific security measures, such as encryption techniques like end-to-end and homomorphic encryption, authentication mechanisms including user authentication and multi-factor authentication, and access control models like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). Integrity verification is addressed through digital signatures and blockchain technology, offering insights into ensuring the integrity of video content during transit. Case studies and implementation examples highlight successful instances of secure video streaming in the cloud, while lessons learned from these cases inform best practices. Future directions anticipate the impact of emerging technologies like AI and quantum computing on video streaming security, alongside identifying research challenges that warrant further investigation. The conclusion succinctly summarizes key findings, and future prospects offer recommendations for ongoing research and development. The comprehensive coverage is supported by a robust reference section citing relevant scholarly sources, providing a solid foundation for understanding and advancing secure video streaming in cloud environments.

2. Security Challenges in Cloud Video Streaming

2.1 Unauthorized Access:

Unauthorized access is a significant security challenge in cloud video streaming. The risks associated with unauthorized access include:

Content Piracy: Hackers may gain unauthorized access to the streaming platform and pirate video content, redistributing it without the consent of content providers. This not only leads to financial losses for content creators but also undermines the business model of streaming services.

Account Hijacking: Cybercriminals may attempt to compromise user accounts, gaining access to sensitive information and video libraries. This can result in unauthorized viewing, sharing, or deletion of content.

Credential Stuffing: Attackers often use previously leaked username and password combinations to gain unauthorized access to user accounts. This highlights the importance of strong authentication mechanisms to prevent unauthorized access.
Insider Threats: Malicious insiders, such as disgruntled employees or contractors with access to the streaming service infrastructure, may intentionally leak or manipulate video content.

2.2 Data Integrity:

Ensuring the integrity of video data during transmission and storage is crucial to maintaining the quality and trustworthiness of the content. Potential threats include:
Man-in-the-Middle Attacks: Attackers may intercept and alter video streams during transmission, leading to degraded quality or the insertion of malicious content. Encryption and secure transmission protocols (e.g., HTTPS) help mitigate these risks.
Data Corruption: Errors in storage or transmission can lead to data corruption, impacting the quality and playback of video content. Regular integrity checks, error detection, and correction mechanisms are essential to mitigate this risk.
Malware Attacks: Malicious software can infect video files, causing corruption or manipulation. Implementing robust antivirus and anti-malware measures is crucial for protecting video content integrity.

2.3 Privacy Concerns:

Privacy concerns in cloud-based streaming services involve both user data and the content itself:
User Data Privacy: Streaming platforms collect vast amounts of user data for personalization and analytics. Privacy concerns arise when this data is mishandled, leading to unauthorized access, data breaches, or inappropriate use. Strict data protection measures and compliance with regulations like GDPR are essential.
Content Privacy: Video content may contain sensitive or private information. Unauthorized access to this content can result in privacy violations. Content encryption, access controls, and secure user authentication are crucial to protect the privacy of video content.
Geolocation and Tracking: The collection and misuse of user location data raise privacy issues. Streaming services should be transparent about their data collection practices and provide users with options to control or opt-out of such tracking.
Addressing these security challenges [20] requires a holistic approach, combining encryption, access controls, regular security audits, and user education to ensure a secure and trustworthy cloud video streaming environment.

3. Encryption Techniques

3.1 End-to-End Encryption:

End-to-End Encryption (E2EE) is a cryptographic technique that ensures the confidentiality of data by encrypting [4, 18] it on the sender's device and only decrypting it on the recipient's device. In the context of video streaming, E2EE provides the following advantages:
Confidentiality: E2EE ensures that video content remains confidential throughout its transmission. Even if intercepted, the encrypted data is unreadable without the proper decryption keys.

Protection Against Man-in-the-Middle Attacks: E2EE mitigates the risk of unauthorized access during data transmission. Even if an attacker intercepts the data, they cannot decipher the content without the encryption keys.

User Privacy: By implementing E2EE, streaming platforms can enhance user privacy. Only users with the appropriate decryption keys can access and view their video content, reducing the risk of unauthorized access.

Content Integrity: E2EE not only protects against unauthorized access but also ensures the integrity of the transmitted data. Any tampering or manipulation during transit would result in decryption failure, alerting users to potential security threats.

Despite its benefits, E2EE can pose challenges for certain streaming features such as server-side processing and content recommendations, as these functionalities require access to the unencrypted content. Balancing security with the need for certain platform features is essential in implementing E2EE effectively.

3.2 Homomorphic Encryption:

Homomorphic encryption [15] is an advanced cryptographic technique that allows computations to be performed on encrypted data without decrypting it first. In the context of video processing in the cloud, homomorphic encryption offers several advantages:

Secure Video Processing: Homomorphic encryption enables the cloud to perform computations on encrypted video data without having access to the unencrypted content. This allows for secure video processing, such as transcoding, analysis, or other operations, while maintaining the confidentiality of the content.

Privacy-Preserving Analytics: Streaming platforms can perform analytics on user behavior or video content without exposing sensitive information. Homomorphic encryption allows for computations on encrypted data, ensuring that the results remain confidential.

Data Outsourcing: Homomorphic encryption enables users to outsource video processing tasks to the cloud without compromising the privacy of their content. The cloud service provider can perform computations on the encrypted data without having access to the plaintext.

However, homomorphic encryption comes with computational overhead and complexity, making it resource-intensive. Striking a balance between security and performance is crucial when implementing homomorphic encryption in a cloud video streaming environment. Additionally, advancements in homomorphic encryption techniques and hardware capabilities may address some of these challenges over time.

4. Authentication Mechanisms

4.1 User Authentication:

User authentication [6] is a critical component of securing access to video streaming services in the cloud. Various methods can be employed to authenticate users and devices:

Username and Password: This is a common and foundational method. Users enter a unique username and a secret password to verify their identity. However, it is susceptible to risks such as password breaches, phishing attacks, and brute force attempts. Implementing strong password policies and using secure password hashing mechanisms can enhance security.

Biometric Authentication: Utilizing biometric data such as fingerprints, facial recognition, or iris scans can provide a more secure and user-friendly authentication method. Biometrics are difficult to forge and enhance the overall user experience, but they may raise privacy concerns and can be subject to certain attacks.

Two-Factor Authentication (2FA): In addition to a password, 2FA requires users to provide a second form of authentication, often through a temporary code sent to a mobile device or generated by an authenticator app. This adds an extra layer of security, reducing the risk of unauthorized access even if passwords are compromised.

Device Authentication: Ensuring that devices are authenticated before accessing the streaming service adds an extra layer of security. This can involve registering and verifying devices, such as through device fingerprints or certificates.

Single Sign-On (SSO): SSO allows users to access multiple services with a single set of credentials. While convenient, it introduces a single point of failure. Implementing SSO securely requires robust protocols like OAuth 2.0 and OpenID Connect.

4.2 Multi-Factor Authentication:

Multi-Factor Authentication (MFA) enhances security by requiring users to provide two or more forms of authentication before accessing the video streaming service. This method significantly reduces the risk of unauthorized access and enhances overall security:

Something You Know (Knowledge): This is typically a password or PIN that the user knows.

Something You Have (Possession): This involves a physical device, such as a mobile phone or a hardware token, which generates a one-time code.

Something You Are (Biometrics): This includes fingerprint scans, facial recognition, or other biometric data.

Benefits of MFA in video streaming security include:

Mitigation of Credential Theft: Even if a user's password is compromised, an additional authentication factor is required, reducing the risk of unauthorized access.

Enhanced Security Without Significant User Burden: MFA adds an extra layer of security without significantly inconveniencing users, especially when using push notifications or authenticator apps.

Compliance with Security Standards: MFA is often a requirement for compliance with security standards and regulations, such as PCI DSS or GDPR.

Implementing user authentication and MFA together creates a robust defense against unauthorized access to video streaming services, enhancing both user and content security in the cloud.

5. Access Control Models

5.1 Role-Based Access Control (RBAC):

Role-Based Access Control (RBAC) [17, 5] is a widely used access control model that regulates access to resources based on roles assigned to users. In the context of video content in cloud environments, RBAC can be implemented effectively:

Roles and Permissions: Users are assigned specific roles, and each role has predefined permissions. For instance, roles could be defined for regular users, content creators, administrators, etc. Permissions associated with each role determine the actions users can perform on video content, such as viewing, uploading, or editing.

Scalability: RBAC is scalable and well-suited for environments with a large number of users. As new users join or roles change, administrators can easily manage access by adjusting role assignments.
Simplicity and Manageability: RBAC simplifies access control by grouping users based on their responsibilities. This makes it easier to manage permissions and ensures that users have the necessary access rights to perform their tasks.
Enforcement of Least Privilege Principle: RBAC supports the principle of least privilege, ensuring that users only have the minimum level of access required to perform their job functions. This reduces the risk of unauthorized access or accidental misuse.
However, RBAC may struggle with handling complex access control scenarios that require more fine-grained control over permissions. Additionally, it may not accommodate dynamic changes in access requirements as effectively as other models.

5.2 Attribute-Based Access Control (ABAC):

Attribute-Based Access Control (ABAC) is a more flexible access control model that considers various attributes to make access decisions. In the context of video streaming in the cloud, ABAC offers the following advantages:
Dynamic Access Control: ABAC allows for dynamic access control decisions based on multiple attributes such as user roles, location, time of access, and other contextual factors. This flexibility is particularly valuable in scenarios where access requirements are dynamic.
Policy-Based Access Control: ABAC relies on policies that define access rules based on attributes. These policies can be adjusted and extended without modifying the underlying system, providing a high degree of adaptability.
Fine-Grained Control: ABAC enables fine-grained control over access by considering a wide range of attributes. This is beneficial for scenarios where different users or groups may require distinct access levels to specific video content.
Compliance and Regulation: ABAC is well-suited for addressing compliance requirements and regulations by allowing organizations to define access policies that align with specific security and privacy standards.
However, the complexity of defining and managing attributes and policies in ABAC can be a challenge. Additionally, ensuring consistent and standardized attribute definitions across the organization is crucial for effective implementation.
In summary, RBAC is effective for straightforward access control scenarios with predefined roles, while ABAC provides greater flexibility and adaptability for dynamic and complex access control requirements in cloud-based video streaming services. The choice between the two models depends on the specific needs and complexity of the environment.

6. Integrity Verification

6.1 Digital Signatures:

Digital signatures play a crucial role in ensuring the integrity of video content during transit. Here's an analysis of their use in this context:
Verification of Content Origin: Digital signatures provide a means to verify the authenticity and origin of video content. When a video is digitally signed, it indicates that the content has not been tampered with and that it originates from a legitimate source.

Data Integrity Assurance: By applying digital signatures to video files, content providers can ensure that the data remains unchanged during transmission. Any modification to the video file, whether accidental or malicious, would result in the signature verification process failing, alerting both the sender and receiver to potential integrity issues.

Authentication of Sender: Digital signatures not only ensure the integrity of the content but also authenticate the identity of the sender. This helps in preventing unauthorized parties from injecting or altering video content during transit.

Non-Repudiation: Digital signatures provide non-repudiation, meaning that the sender cannot later deny sending the content. This is important for legal and accountability reasons, especially in the context of video content distribution.

However, the effectiveness of digital signatures relies on the secure management of private keys. If a private key is compromised, it could be used to create fraudulent digital signatures. Key management practices, such as using hardware security modules (HSMs), are crucial to mitigate this risk.

6.2 Blockchain Technology:

Blockchain technology has the potential to establish an immutable record of video stream transactions, ensuring integrity and traceability:

Immutability: Once recorded on a blockchain, transactions, including the details of video streams, are almost impossible to alter. This immutability ensures the integrity of the recorded data.

Decentralization: The decentralized nature of blockchains reduces the risk of a single point of failure. Video stream transactions recorded on a blockchain are distributed across nodes, making it challenging for malicious actors to compromise the entire system.

Transparency and Traceability: Blockchain provides a transparent and auditable record of all transactions. This can be valuable for tracking the history of video streams, identifying any unauthorized changes, and ensuring compliance with content distribution agreements.

Smart Contracts: Smart contracts, self-executing contracts with the terms of the agreement directly written into code, can automate certain processes in video streaming, such as royalty payments or access permissions, enhancing efficiency and reducing the risk of disputes.

However, challenges such as scalability, energy consumption (in the case of some consensus algorithms like Proof-of-Work), and regulatory considerations need to be addressed when implementing blockchain in the video streaming domain. Additionally, blockchain may be more suitable for use cases where the benefits of decentralization and immutability outweigh the associated complexities and costs.

7. Case Studies and Implementation Examples

7.1 Successful Implementations:

Netflix:

Security Measures: Netflix employs a combination of encryption, secure APIs, and digital rights management (DRM) to protect its vast library of video content.

Adaptive Streaming: Netflix utilizes adaptive streaming technologies to deliver content based on the viewer's network conditions, ensuring a seamless and secure streaming experience.

Global Content Delivery: Netflix leverages a global content delivery network (CDN) to optimize streaming performance and reduce latency.

Disney+: Multi-DRM Approach: Disney+ employs a multi-DRM strategy to protect content across various devices. This includes using industry-standard encryption and DRM solutions.
User Authentication: Disney+ incorporates robust user authentication mechanisms, including multi-factor authentication, to ensure secure access to user accounts and prevent unauthorized viewing.
Content Recommendations: While ensuring security, Disney+ uses personalized content recommendations to enhance user experience, striking a balance between security and user engagement.
Vimeo:
Secure Video Sharing: Vimeo provides secure video sharing for businesses and professionals. It includes features like password protection, domain-level privacy, and customizable embed settings to control access to videos.
Advanced Analytics: Vimeo offers analytics tools that provide insights into who is watching the videos, helping content creators understand their audience without compromising viewer privacy.

7.2 Lessons Learned:
Continuous Monitoring and Updates:
Lesson: Implement continuous monitoring to detect and respond to security threats in real-time.
Insight: Regularly updating security measures based on emerging threats and vulnerabilities is crucial for maintaining a robust defense against evolving risks.
User Education and Awareness:
Lesson: Educate users about best security practices and potential risks associated with video streaming services.
Insight: User awareness can be a powerful defense against social engineering attacks and unauthorized access. Implementing educational programs can help users make informed decisions.
Balancing Security and User Experience:
Lesson: Strive to achieve a balance between robust security measures and a seamless user experience.
Insight: While security is paramount, overly complex or intrusive security measures may negatively impact the user experience. Finding a balance is essential for user satisfaction.
Adopting Industry Standards:
Lesson: Adhere to industry standards and best practices for encryption, authentication, and access control.
Insight: Industry standards provide a foundation for building secure systems. Adherence to standards ensures compatibility and interoperability with other services and technologies.
Agile and Adaptive Security Measures:
Lesson: Implement security measures that can adapt to evolving threats and technological changes.
Insight: The dynamic nature of cybersecurity requires an agile approach to security measures. Regularly assess and update security protocols to stay ahead of emerging threats.
Collaboration and Information Sharing:
Lesson: Foster collaboration and information sharing within the industry to address common security challenges.
Insight: Sharing insights and best practices among industry players can enhance collective security. Collaborative efforts can lead to the development of standardized security protocols.

These lessons from successful implementations emphasize the importance of a holistic and adaptive approach to secure video streaming services in the cloud. Continual learning, collaboration, and a user-centric focus contribute to the development of resilient and user-friendly security solutions.

8. Future Directions

8.1 Emerging Technologies:

Artificial Intelligence (AI):

Content Analysis and Recognition: AI can enhance content analysis and recognition, enabling more effective identification of copyrighted material, detection of inappropriate content, and ensuring compliance with content distribution regulations.

Behavioral Analytics: AI-driven behavioral analytics can be employed to detect unusual patterns of user behavior, aiding in the identification of potential security threats or account compromises.

Dynamic Security Response: AI can contribute to dynamic security response mechanisms, automatically adapting security measures based on real-time analysis of streaming patterns and potential threats.

Quantum Computing:

Impact on Encryption: The development of quantum computing poses a potential threat to traditional encryption algorithms. Quantum-resistant encryption methods may become necessary to maintain the security of video content in the future.

Secure Key Distribution: Quantum key distribution (QKD) offers a more secure method for distributing cryptographic keys, providing a potential solution to the challenges posed by quantum computing advancements.

Blockchain and Decentralized Technologies:

Immutable Video Provenance: Blockchain can be utilized to establish an immutable record of video provenance, ensuring the authenticity and integrity of video content from creation to distribution.

Decentralized Content Delivery Networks (CDNs): Decentralized CDNs, enabled by blockchain and distributed ledger technologies, could enhance the scalability and resilience of content delivery.

5G Technology:

Low Latency Streaming: The widespread adoption of 5G technology can significantly reduce latency, enabling low-latency video streaming. This not only improves user experience but also introduces new security challenges that need to be addressed.

Edge Computing:

Distributed Video Processing: Edge computing can be leveraged for distributed video processing, reducing the need to transmit large amounts of video data to central servers. This introduces opportunities for improved privacy and security by processing data closer to its source.

8.2 Research Challenges:

Post-Quantum Cryptography:

Challenge: The development and implementation of post-quantum cryptographic algorithms to secure video content against potential threats posed by quantum computing.

Importance: As quantum computing matures, there is a need to ensure that encryption methods used to protect video content remain secure.

Explainable AI in Security:
Challenge: Developing AI models for security purposes that are explainable, transparent, and can be audited to ensure accountability and compliance.
Importance: Understanding and trusting the decisions made by AI systems is crucial, especially in security-sensitive applications where accountability is essential.
Privacy-Preserving AI:
Challenge: Ensuring that AI-driven analytics and processing of video content respect user privacy and comply with data protection regulations.
Importance: As AI becomes more integrated into video streaming services, maintaining user privacy is paramount to build and maintain user trust.
Standardization in Blockchain Integration:
Challenge: Establishing industry standards for the integration of blockchain and decentralized technologies into video streaming services.
Importance: Standardization facilitates interoperability, ensures consistency, and promotes widespread adoption of secure blockchain-based solutions.
Dynamic Security Adaptation:
Challenge: Developing systems that can dynamically adapt security measures in real-time based on evolving threats and streaming patterns.
Importance: As the threat landscape evolves, security measures must be agile and responsive to effectively protect video streaming services.
Secure Edge Computing:
Challenge: Ensuring the security of video processing at the edge, especially in decentralized environments where edge devices play a significant role.
Importance: Edge computing introduces new security considerations, and addressing these challenges is crucial to leverage the benefits of distributed video processing.
Addressing these research challenges and embracing emerging technologies will be crucial for the continued improvement of security in cloud-based video streaming services, ensuring that they remain resilient and adaptive in the face of evolving threats and technological advancements.

9. Conclusion

In this comprehensive review of security challenges, technologies, and implementations in cloud-based video streaming, several key findings have emerged:
Security Challenges: Unauthorized access, data integrity, and privacy concerns pose significant challenges in the realm of cloud-based video streaming. Addressing these challenges requires a multi-faceted approach that incorporates encryption, access controls, and user authentication mechanisms.
Encryption Techniques: End-to-end encryption and homomorphic encryption stand out as crucial techniques for ensuring the confidentiality and integrity of video content. These methods play pivotal roles in protecting data during transmission, processing, and storage.
Authentication Mechanisms: User authentication and multi-factor authentication are fundamental for controlling access to video streaming services. Balancing security with user experience is essential, and advancements in authentication technologies, such as biometrics, contribute to enhanced security measures.

Access Control Models: Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) offer different approaches to managing access, each with its strengths. RBAC simplifies access control based on predefined roles, while ABAC provides flexibility by considering dynamic attributes.

Integrity Verification: Digital signatures and blockchain technology contribute significantly to ensuring the integrity of video content. Digital signatures authenticate the origin and ensure data integrity, while blockchain provides an immutable record of transactions, enhancing transparency and traceability.

Successful Implementations: Case studies of successful implementations by streaming platforms like Netflix, Disney+, and Vimeo illustrate the effectiveness of combining encryption, secure user authentication, and adaptive streaming technologies to deliver a secure and user-friendly experience.

Looking ahead, future research and development in secure video streaming in the cloud should focus on the following areas:

Quantum-Safe Cryptography: With the advent of quantum computing, there is a need to explore and develop quantum-resistant cryptographic algorithms to secure video content against potential threats.

Explainable AI and Privacy-Preserving Techniques: Enhancing AI-driven analytics for security purposes by making them more explainable and ensuring they adhere to privacy-preserving principles. This is crucial for gaining user trust and complying with data protection regulations.

Integration of Emerging Technologies: Research should explore the seamless integration of emerging technologies, such as 5G, edge computing, and blockchain, into video streaming services. This includes standardizing the use of blockchain for content provenance and ensuring secure video processing at the edge.

Dynamic Security Adaptation: Developing adaptive security systems that can dynamically adjust to evolving threats and streaming patterns in real-time. This requires continuous monitoring, threat intelligence integration, and the ability to respond proactively to emerging security challenges.

User-Centric Security Measures: Future developments should prioritize user-centric security measures that balance robust protection with a seamless and positive user experience. This includes user education programs and the implementation of intuitive security features.

In conclusion, the landscape of secure video streaming in the cloud is dynamic and evolving. By addressing these future prospects, the industry can continue to innovate, adapt, and provide secure, reliable, and user-friendly video streaming services in the ever-changing digital landscape.

10. References

1. Chen K, Hoque R, Dharmarajan K, LLontop E, Adebola S, Ichnowski J, Kubiatowicz J, Goldberg K. FogROS2-SGC: A ROS2 Cloud Robotics Platform for Secure Global Connectivity. arXiv preprint arXiv:2306.17157. 2023 Jun 29.
2. Darwich M, Khalil K, Ismail Y, Bayoumi M. Enhancing cloud-based video streaming efficiency using neural networks. In2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS) 2023 Jul 23 (pp. 1-5). IEEE.
3. Farahani R, Bentaleb A, Timmerer C, Shojafar M, Prodan R, Hellwagner H. SARENA: SFC-Enabled Architecture for Adaptive Video Streaming Applications. InICC 2023-IEEE International Conference on Communications 2023 May 28 (pp. 864-870). IEEE.
4. Fouzar Y, Lakhssassi A, Ramakrishna M. A Novel Hybrid Multikey Cryptography Technique for Video Communication. IEEE Access. 2023 Feb 6;11:15693-700.

5. He Y. BLOCKCHAIN-BASED ACCESS AND USAGE CONTROL OF CLOUD-BASED DIGITAL TWINS (Doctoral dissertation, University of Saskatchewan).
6. Jiang X, Dou R, He Q, Zhang X, Dou W. EdgeAuth: An intelligent token-based collaborative authentication scheme. Software: Practice and Experience. 2023.
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, Goodridge W. Reinforcement Learning in DASH. International Journal of Advanced Networking and Applications. 2020 Mar 1;11(5):4386-92.
13. Khan K. A Framework for Meta-Learning in Dynamic Adaptive Streaming over HTTP. International Journal of Computing. 2023 Apr;12(2).
14. Li X, Darwich M, Salehi MA, Bayoumi M. A survey on cloud-based video streaming services. InAdvances in Computers 2021 Jan 1 (Vol. 123, pp. 193-244). Elsevier.
15. Mahato GK, Chakraborty SK. A comparative review on homomorphic encryption for cloud security. IETE Journal of Research. 2023 Sep 20;69(8):5124-33.
16. Narayanan KL, Naresh RJ. An efficient key validation mechanism with VANET in real-time cloud monitoring metrics to enhance cloud storage and security. Sustainable Energy Technologies and Assessments. 2023 Mar 1;56:102970.
17. Roslin Dayana K, Shobha Rani P. Trust aware cryptographic role based access control scheme for secure cloud data storage. Automatika. 2023 Oct 2;64(4):1072-9.
18. Saini P, Kumar K. S-method: secure multimedia encryption technique in cloud environment. Multimedia Tools and Applications. 2023 Jun 16:1-5.
19. Usman M, He X, Lam KM, Xu M, Bokhari SM, Chen J. Frame interpolation for cloud-based mobile video streaming. IEEE Transactions on Multimedia. 2016 Mar 2;18(5):831-9.
20. Viola I, Cesar P. Volumetric video streaming: Current approaches and implementations. Immersive Video Technologies. 2023 Jan 1:425-43.