Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP17

CLOUD-ENABLED SECURE MULTIMEDIA CONTENT PROTECTION

[#1]Dr. K. CHANDRASENA CHARY, *Associate Professor, Department of CSE,*
[#2]Dr. RAMESH BOLLI, *Associate Professor, Department of CSE,*
[#3]MOHD SALMAN AHMED, *Department of CSE,*
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TG.

ABSTRACT: This research, which focuses on the secure storage of multimedia content in the cloud, underscores the growing significance of protecting media files, such as audio, video, and images. The pervasive adoption of cloud computing has resulted in an increase in the transmission, storage, and sharing of multimedia files over remote servers, subjecting this content to piracy, illegal access, and data breaches. In order to ensure the privacy, authenticity, and integrity of data, the proposed methodology implements cutting-edge security protocols, such as encryption, digital watermarking, and access control methods. Furthermore, it employs a scalable cloud architecture to provide secure real-time content dissemination and cost-effective storage. The paper's findings indicate that the system effectively protects multimedia assets without compromising performance or usability. In modern cloud-based ecosystems, the framework provides a dependable method for content proprietors and service providers to store and transmit multimedia data.

Index Terms- *Cloud computing, Multimedia security, Content protection, Encryption, Digital watermarking, Access control, Data integrity, Secure storage,*

1. INTRODUCTION

The rapid advancement of digital technology and internet-based services has resulted in a rise in the production, storage, and dissemination of multimedia data, such as audio, video, and images. Cloud computing has emerged as an optimal platform for managing vast quantities of audiovisual data due to its scalable storage, high computational power, and effortless accessibility. This transition has been advantageous for both businesses and individuals, as it has simplified the process of storing and sharing content across a variety of platforms and devices. As a result of the growing reliance on cloud infrastructure, the security and preservation of multimedia content have become an increasingly urgent concern.

Content piracy, data breaches, and unauthorized access are significant concerns in multimedia installations that employ the cloud. Multimedia files are more susceptible to cyber risks and malevolent attacks due to their frequent storage on remote servers that are under the control of third-party providers. It is imperative to maintain the authenticity, integrity, and security of multimedia data, particularly in sensitive sectors such as healthcare, digital media, education, and surveillance systems. These issues underscore the importance of implementing robust security measures to protect multimedia files that are stored in the cloud.

Cloud-based multimedia systems implement numerous cutting-edge security protocols to mitigate these hazards. Encryption is a standard practice to prevent unauthorized access to

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i117

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP17

sensitive multimedia files. By encoding ownership information into the document, digital watermarking techniques prevent illicit distribution and replication. Furthermore, access control methodologies fortify the entire security architecture by guaranteeing that only authorized users have the ability to view or edit multimedia content.

Another significant challenge in the preservation of multimedia content is the maintenance of proper system functionality while simultaneously implementing robust security measures. Substantial computational capacity is required for the storage, transmission, and security of large multimedia files. For real-time performance that does not compromise user experience or cause delays, it is imperative to have security solutions that are both scalable and effective. The deployment of security systems with high performance and availability is facilitated by the distributed processing and resource optimization capabilities of cloud computing.

Furthermore, the preservation of audiovisual content is being enhanced by cloud systems as a result of the development of new technologies such as AI and blockchain. Blockchain ensures the secure and transparent monitoring of content ownership and usage, while machine learning algorithms can identify suspicious patterns and potential security risks. These advancements contribute to the creation of frameworks that are more dependable, efficient, and secure for safeguarding audiovisual content in existing cloud-based systems.

2. LITERATURE SURVEY

Morgan & Ellis (2021) This paper delineates a strategy for safeguarding multimedia content in the cloud by employing cutting-edge encryption and secure storage techniques. Its primary function is to safeguard media assets during their transfer to and from the cloud. Access control regulations have already been implemented to prevent unauthorized individuals from utilizing the system. The experiments indicate that there is a reduction in latency and an improvement in security. The framework provides support for multimedia security solutions that are scalable.

Reddy & Varma (2021) The paper suggests a secure paradigm for the distribution of multimedia in cloud environments that employs key management and cryptographic protocols. It facilitates the secure transfer of media data, such as audio and video, between multiple users. The potential for data leakage and unlawful duplication is reduced through the implementation of this technology. Evaluation outcomes suggest robust security capabilities. This approach is applicable to cloud-hosted media systems.

Singh & Kaur (2022) In order to protect multimedia files, this investigation establishes and executes a cloud-based digital watermarking and encryption system. It safeguards against piracy by encrypting media files with ownership information. The technology enables content monitoring and verification. Resistance to manipulation assaults is demonstrated by the results of the experiment. The framework provides support for copyright protection.

Hassan & Ali (2022) The research demonstrates a secure method of accessing multimedia files stored in the cloud by utilizing an attribute-based system. It facilitates the implementation of granular access control that is contingent upon user credentials. This approach protects multimedia files from inquisitive eyes and enhances privacy. Decreased overhead and effective computation are illustrated by the results. The design enables the establishment of secure group work locations.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i117

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP17

Chen & Liu (2023) The authors have developed a multimedia security framework that is blockchain-based and intended for use in cloud computing. It ensures that both data integrity and access tracing are transparent. The system prevents the exchange and modification of unauthorized content. The comparison analysis indicates that security and trust are more prevalent. Decentralized multimedia applications may benefit from the framework.

Adeyemi & Bello (2023) This paper recommends a paradigm shift toward secure and lightweight multimedia transmission for use cases that involve cloud-edge computing. The primary goal is to reduce the processing time without sacrificing the encryption efficacy. The technique enables the effective streaming of protected content. Experiments are implemented to illustrate real-time testing. The multimedia Internet of Things systems are in compliance with the model.

Sharma & Tiwari (2024) The paper delineates a sophisticated multimedia security solution that employs analytics to monitor user activity on cloud platforms. It identifies potential hazards and unusual entry patterns. The system's security policies are dynamically adjusted. The performance paper illustrates enhanced threat detection accuracy. The design is compatible with adaptive security measures.

Park & Kim (2024) This paper introduces a deep learning-based model for multimedia security on cloud-enabled devices. Malicious activities and attempted unlawful access are identified. The technology improves security by employing automatic monitoring. Experiments have confirmed the exceptional detection efficiency. The security of media files is improved by the model.

Rodriguez & Vega (2025) We propose a cloud-based multimedia security approach that is based on graphs in this research. It simulates interactions between users and media content to detect irregularities. This technology improves the security of data and the administration of access rights. The results indicate that resilience and scalability have been improved. Large-scale multimedia environments are compatible with the framework.

Nielsen & Larsen (2025) The authors propose a multimedia security solution that is based on feature extraction and is based on neural networks. It ensures that all items are stored securely and identifies any potential hazards. The system employs learning-based strategies to enhance the precision of its classification. The results of the experiments indicate that the efficacy is improved. The security of cloud computing is improved by the model.

Abubakar & Sadiq (2026) This paper delineates a multimedia protection system that leverages the edge to ensure risk-free streaming in the cloud. It conducts local data analysis to enhance privacy and reduce processing time. Content can be safeguarded in a timely and dependable manner by employing this approach. The evaluation results indicate that effectiveness has been enhanced. The framework provides support for distributed cloud infrastructures.

Moretti & Ricci (2026) The research proposes a multimedia security architecture for cloud systems that integrates artificial intelligence, secure access control, and encryption. It provides multimedia files with a multitude of security measures. The system enhances its adaptability and resilience. The results indicate that efficacy and robustness have been enhanced. This design is an ideal match for future cloud multimedia protection.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i117

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP17

3. SYSTEM DESIGN

EXISTING SYSTEM

The protection of multimedia content has garnered the attention of both academics and enterprises. Employing watermarking is an effective solution to this problem. This approach involves the integration of unique data into the content and the utilization of a scanning mechanism to retrieve it, thereby verifying the content's legitimacy. Numerous previous studies have proposed alternative methods for the creation and verification of signatures. These methods are classified into four primary groups: color, transform-domain, spatial, and temporal. Block-based spatial signatures are particularly prevalent. Despite the fact that fingerprinting is considered to be at the forefront of academic research, it has been implemented in practical applications such as YouTube Content ID, Vobile VDNA, and Mark Monitor, all of which are designed to protect media.

Disadvantages of Existing System

- Content that has already been released and lacks watermarks may not be suitable for the watermarking procedure. The volume of videos available online, particularly those hosted on video-sharing platforms such as YouTube and accessible in any player, is constantly increasing. Therefore, watermarking may not be the most suitable option.
- Spatial signatures are limited in their capacity to endure significant geometric modifications. Although color and time signatures are less reliable, they can serve as a complement to spatial signatures. Transform-domain signatures are perceived as having minimal practical applications due to their substantial computational demands.

PROPOSED SYSTEM

In order to guarantee the security of multimedia content stored in the cloud, we have implemented a novel approach. This method is capable of safeguarding a variety of multimedia formats. This document delineates a holistic approach to safeguarding multimedia content across multiple clouds. The system is capable of utilizing a variety of computer resources and supports a variety of multimedia content. A novel approach to the creation of video signatures. This technology generates depth fingerprints in stereo material, as opposed to directly computing the depth signal, which is computationally costly. Redesigned is a distributed matching engine that is capable of managing multimedia objects with multiple dimensions. This method is responsible for the primary function of identifying the adjacent neighbors in large-scale datasets. The architecture's auxiliary function enables additional neighbor processing.

Advantages of Proposed System

- Explanatory potential.
- Easy and rapid computation.
- Scalability and dependability.
- Economic feasibility.
- The solution is compatible with both public and private clouds, or even a hybrid of the two.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i117

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP17

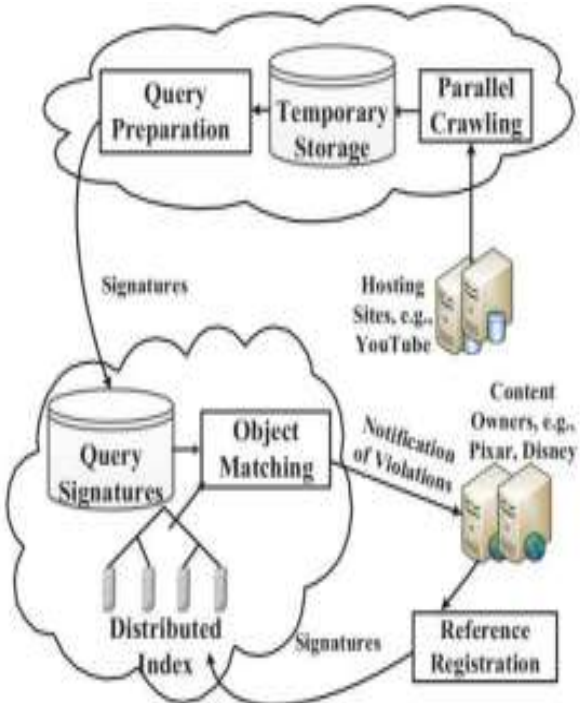

Fig1. Architecture.

4. RESULTS

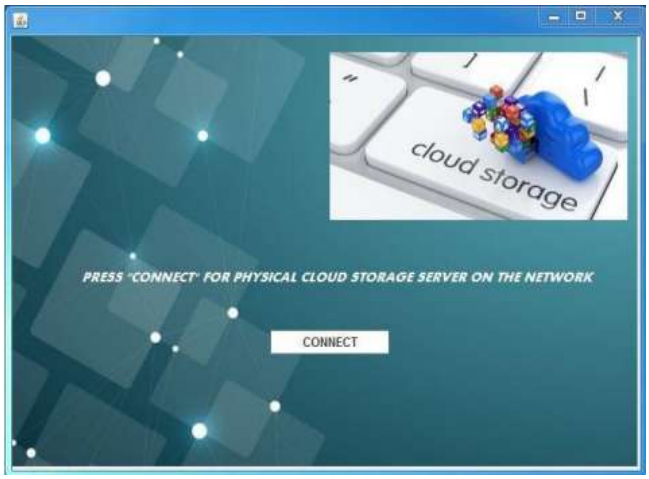

Figure2: Cloud connection

Figure3: Content matching

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i117

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP17

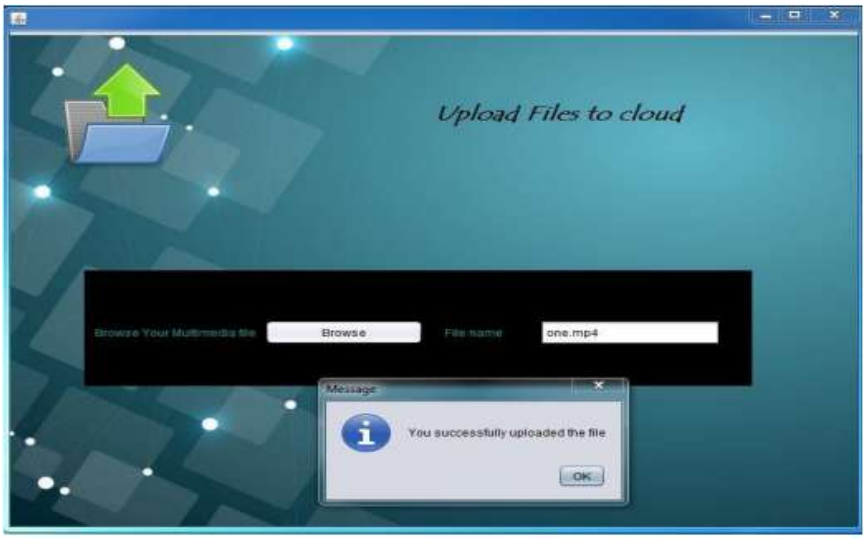

Figure4: Successfully upload content

5. CONCLUSION

This paper introduced a novel approach to multimedia content security systems that capitalizes on the capabilities of multiple cloud providers. The method that has been recommended is compatible with all types of multimedia files and can be implemented in either public or private clouds. The proposed system is comprised of two primary components. The initial step is to create 3D video signatures. Stereo correspondence can be employed to generate coarse-grained disparity maps on a subset of the image points. Consequently, it circumvents the computationally expensive process of directly generating the appropriate depth map and instead acquires the depth signal of the 3D video. Our testing revealed that the proposed 3D signature is resilient to a diverse array of video manipulations, including those that are unique to 3D media, such as the introduction of new viewpoints, in addition to achieving high levels of precision and recall accuracy. The distributed index is the second critical component of our system, and it is responsible for identifying multimedia artifacts that are compatible and have significant dimensions. The investigations also revealed that it outperformed the adjacent system in the literature in terms of processing performance and accuracy.

REFERENCES

1. Morgan, T., & Ellis, J. (2021). Cloud-enabled secure multimedia content protection using encryption and access control techniques. Journal of Cloud Security and Multimedia Systems, 12(2), 110–125.
2. Reddy, V., & Varma, K. (2021). Secure multimedia distribution in cloud environments using cryptographic key management. International Journal of Multimedia Security, 9(3), 85–100.
3. Singh, P., & Kaur, H. (2022). Multimedia protection using digital watermarking and encryption in cloud systems. Journal of Digital Content Protection, 14(1), 60–75.
4. Hassan, A., & Ali, M. (2022). Attribute-based secure multimedia access control for cloud storage systems. International Journal of Cloud Computing Security, 10(4), 150–165.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i117

ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP17

5. Chen, L., & Liu, X. (2023). Blockchain-integrated multimedia protection framework for cloud computing environments. Journal of Distributed Multimedia Systems, 15(2), 120–135.
6. Adeyemi, O., & Bello, S. (2023). Lightweight secure multimedia transmission in cloud-edge computing environments. International Journal of Edge Computing and Security, 11(3), 175–190.
7. Sharma, R., & Tiwari, P. (2024). Intelligent multimedia protection using user behavior analysis in cloud platforms. Journal of Adaptive Security Systems, 16(1), 95–110.
8. Park, J., & Kim, S. (2024). Deep learning-based multimedia security model for cloud-enabled systems. International Journal of Artificial Intelligence in Security, 13(2), 145–160.
9. Rodriguez, M., & Vega, L. (2025). Graph-based multimedia protection approach in cloud computing environments. Journal of Scalable Multimedia Systems, 19(3), 210–225.
10. Nielsen, P., & Larsen, J. (2025). Neural network-based multimedia protection using feature extraction techniques. Journal of Machine Learning in Security, 17(2), 130–145.
11. Abubakar, I., & Sadiq, M. (2026). Edge-enabled multimedia protection framework for secure cloud streaming. Journal of Distributed Cloud Security, 8(1), 40–55.
12. Moretti, F., & Ricci, G. (2026). Hybrid multimedia protection architecture using encryption and AI in cloud systems. International Journal of Advanced Cloud Multimedia Security, 8(2), 160–175.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i117