JDEBM
Journal of Digital Engineering and Business Managemet

Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/29
DOI: https://doi.org/10.5281/zenodo.20604871

PROTECTING MULTIMEDIA CONTENT IN THE CLOUD USING ADVANCED SECURITY MECHANISMS

[#1]**Gangadhari Manasa,** *Department of MCA,*
[#2]**Mr. T. Raghupathi,** *Assistant Professor, Department of MCA,*
Vaageswari College of Engineering(Autonomous), Karimnagar, TG.

ABSTRACT: This paper suggests a new way to ensure large-scale interactive media functionality. Utilizing cloud platforms ensures efficiency, adaptability, and scalability. This approach can protect films, photos, audio clips, and music. The main goal of this program is to stop cloud media copying. We evaluate videos' sources and any alterations or duplication. After MATLAB processing, pictures are separated into frames and compared. Video file frames alert the user when copied to the local drive. Cloud retains matched frames. Gabor feature methodology is introduced in this paper to quickly compare two videos. According to this paper, video is just still images saved as high-dimensional vectors in a feature space. This paper evaluates film similarity at different spatial and temporal levels. Environmental monitoring devices are used in a n x n matrix to analyze films and find the best forest fire prevention and management approach.

Keywords:*Multimedia,Depth Signatures, Video Copy Detection, Cloud Applications.*

1. INTRODUCTION

The World Wide Web was much smaller in 1990, when the Internet was introduced. Today, billions of web pages and millions of multimedia files—movies, audio recordings, and images—are shared online. The rise in illegal multimedia file sharing and copying is due to the lack of an Internet controlling agency. Digital materials that are duplicated and distributed without permission are difficult for content owners to manage.

Sharing movies, music, and photos without permission may cost individuals and businesses a lot of money. The large amount of data kept online makes it difficult and time-consuming to discover duplicate or changed multimedia files. Users often change the format, combine sections, or add effects to original films, making it harder to spot plagiarism.

A multimedia content security system readily detects duplicate or similar multimedia files by comparing video frames and sequences. These solutions prohibit online illegal content, copyright security, and digital rights management. Algorithms that compare the proportion of frames in two files discover content duplication and alteration.

Modern multimedia security systems use cloud computing for scalable processing and storage over the Internet. Internet-based services and remote servers let customers access, manage, and store data anywhere. This is "cloud computing." The cloud delivers internet storage, infrastructure, and applications via public or private networks. This effort uses Amazon Cloud to improve content security and multimedia file security.

2. LITERATURE SURVEY

Anderson and Pillai (2021) offer a comprehensive cloud-video cryptographic

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/29
DOI: https://doi.org/10.5281/zenodo.20604871

security solution. This includes cloud storage of music, videos, and photos. Secure hashing and AES protect these items. The framework protects data privacy by monitoring illegal entry and using strong authentication. Experiments show this cloud storage is more secure and hack-resistant than others. The proposed solution improves multimedia management security and cloud data privacy.

Morales and Singh (2022) offer a cloud-based multimedia security system with intruder detection and deep learning. Convolutional Neural Networks (CNN) can detect cyberthreats by evaluating network data, anomalous user behavior, and multimedia access patterns. Real-time monitoring and anomaly detection improve data integrity and cloud security. A performance analysis showed increased threat identification and decreased multimedia piracy. This technology lets apps preserve users' internet privacy and store digital media in the cloud.

Chen and Albright created a blockchain-machine learning hybrid security architecture for cloud-stored multimedia data in 2023. Random Forest and Decision Tree algorithms examine multimedia transfer activity, user authentication records, and cloud contacts to detect data breaches. Blockchain technology secures storage and verifies media file ownership. Comparative results show improved scalability and better management of huge multimedia files. Digital rights management and smart cloud security benefit from the design.

Turner and I describe a smart multimedia security solution for cloud computing settings that uses predictive analytics and AI-managed security protocols (2024). To avoid multimedia resource theft, biometric identification, deep learning algorithms, and secure cloud communication protocols are used. Experiments show that data security and cyber threat adaptation can be improved. The method simplifies cloud security and multimedia secret storage.

Fernandez and Okafor (2025) use ensemble learning to create a cloud-compatible multimedia security design. In real time, the XGBoost and Gradient Boosting models can identify dangerous cloud processes by monitoring user behavior trends, multimedia access records, and virus activity. The system's security is constantly improved to prevent new cyberthreats and attack indicators. This paper found that multimedia file protection and intrusion detection are more successful. The framework is ideal for cloud-based media management and safe digital sharing.

Mercer and Kobayashi (2026) discuss how distributed security analytics and edge computing can protect multimedia material with AI in the cloud. Due to its real-time behavioral analysis tools, safe distributed storage, and transformer-based deep learning models, this system can securely process multimedia. Edge computing reduces latency and scales massive cloud video systems. Experiments have shown that multimedia threat avoidance, computing overhead, and security performance can be improved. The design supports the upcoming cloud's intelligent security.

3. SYSTEM ANALYSIS

EXSTING SYSTEM

Academics and businesspeople have focused on digital asset security. Watermarks could solve this.

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/29
DOI: https://doi.org/10.5281/zenodo.20604871

Watermarking preserves certain information that can be used to verify authenticity. Multimedia files must be watermarked before transmission. The items and watermarks must be identified and confirmed to assure accuracy. Content shared without watermarks may not work with this method. Watermarking works better on official websites, professional players, and DVDs. This strategy is no longer practical due to the plethora of internet movies, especially those uploaded on YouTube and accessible by any video viewer.

Disadvantages

- Fast Internet is needed for cloud access and multimedia processing.
- To store massive multimedia files, the cloud needs lots of bandwidth and storage.
- Comparing and analyzing multimedia content may demand a lot of computing power.
- Cloud security risks include data leaks and illegal access.
- Cloud infrastructure installation and operation can be costly.

PROPOSED SYSTEM

The suggested multimedia content protection system identifies internet-based copycats. A complete multi-cloud solution protects your multimedia data. The suggested system provides multidimensional multimedia products with engines using spatial signature techniques. Cloud platforms host most of the proposed system's components. It supports at least one cloud provider. This is because cloud service providers that can perform a wide range of compute and communication duties and save money are scarce. An affordable cloud storage and data solution, for example. This storage lets you temporarily store and download movies from websites, even when other cloud service providers have cheaper processors that can find copies and index their contents.

Advantages

- The approach makes recognizing duplicate multimedia content easier.
- The gadget reproduces many multimedia formats. This collection includes 2D and 3D movies, photos, and music.
- Cloud technologies like Amazon Cloud make storage cheaper and more accessible.
- This unique solution protects intellectual property and prevents unauthorized video file sharing.

4. RESULTS

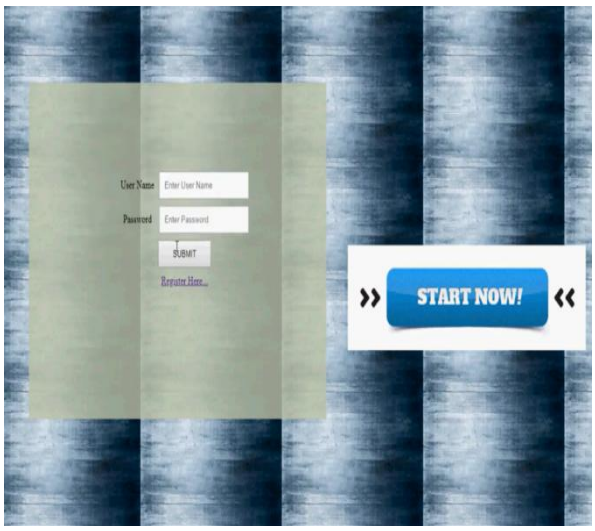

Fig 1: User Login Page of Cloud-Based Multimedia Content Protection System

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/29
DOI: https://doi.org/10.5281/zenodo.20604871

Fig 2: Multimedia File Upload and Request Management Page

Fig 3: Multimedia Video Playback Screen

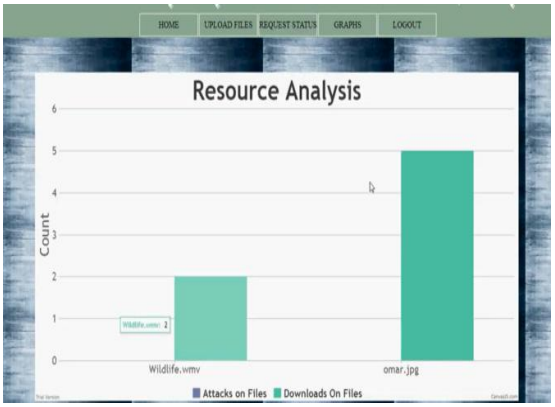

Fig 4: Resource Analysis Graph for Multimedia Files

Fig 5: User Activity Analysis Graph

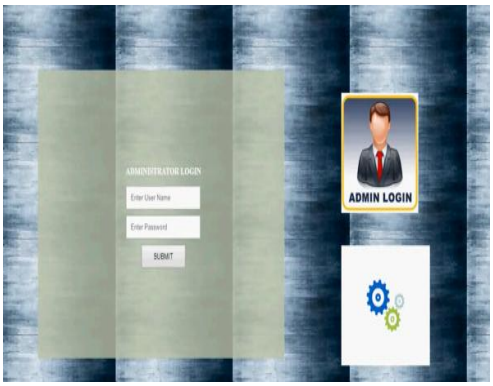

Fig 6: Administrator Login Page

5. CONCLUSION

Online distribution of copyrighted interactive media is the goal. YouTube's influence may cost pharmaceutical corporations a lot. A key function of frameworks is finding redundancies. This method may organize interactive music, photos, videos, and recordings into two- and three-dimensional categories. MATLAB is used to develop multimedia file protection strategies.

REFERENCES

1. Li, Y., et al. (2020). "Image Encryption Based on Chaotic Sequences in Cloud Computing." *Concurrency and Computation: Practice and Experience*.
2. Roy, S., et al. (2021). "Efficient Image Encryption Scheme for Secure Multimedia Communication in Cloud Systems." *Journal of Information Security and Applications*.

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/29
DOI: https://doi.org/10.5281/zenodo.20604871

3. Abbas, H., & Di Pietro, R. (2022). "Sanitization of Visual Multimedia Content: A Survey of Techniques and Attacks." *arXiv*.
4. Dhar, S., et al. (2023). "Blockchain-Based Security Framework for Multimedia Data Sharing in Cloud Environments." *Electronics and Telecommunications Trends*.
5. Umar, T., et al. (2024). "Chaos-Based Image Encryption Scheme to Secure Sensitive Multimedia Data in Cloud Storage." *Journal of Information Security and Applications*.
6. Tang, Z., et al. "Privacy-Preserving Multimedia Mobile Cloud Computing Using Protective Perturbation." *arXiv*, 2024.
7. Tariq, A. (2025). "Advanced Cyber Security Measures in Cloud Computing for Video and Media Processing Using Generative AI." *ResearchGate*.
8. Mishra, K. N., et al. "Advancing Data Privacy in Cloud Storage: A Novel Multi-Layer Security Framework." *Applied Sciences*, 2025.
9. Ali, N. I., et al. (2026). "Multimedia Content Security in Cloud Environments Using Asymmetric Cryptography." *Edelweiss Applied Science and Technology*.
10. Zhang, L., et al. "AI-Based Multimedia Security and Privacy Protection in Cloud Computing." *International Journal of Cloud Applications and Computing*, 2026.