ETDT
Emerging Trends in Digital Transformation
Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-13***

A SECURE MULTIMEDIA PROTECTION MODEL FOR CLOUD STORAGE AND DISTRIBUTION

[#1]**MOHAMMED SALMAN JAWEED,** *Dept of CSE,*
[#2]**MR. S. SATEESH REDDY,** *Associate Professor , Dept of CSE,*
Vaageswari College of Engineering(Autonomous), Karimnagar, TG.

ABSTRACT: A Secure Multimedia Protection Model for Cloud Storage and Distribution ensures the confidentiality, authenticity, and integrity of multimedia content stored in the cloud. Hackers, piracy, data breaches, and manipulation are all at an increased risk as the volume of image, music, and video storage on cloud servers increases. The proposed architecture provides multi-layered security through contemporary encryption, secure key management, digital watermarking, and user identity. Multimedia files can be uploaded, stored, and shared in a secure manner, with ownership tracking. The scalability and computational power savings of this framework render it an optimal choice for large-scale cloud systems. Multimedia management in cloud ecosystems is less susceptible to data intrusions, replay attacks, and unlawful redistribution, as demonstrated by experiments.
Keywords: *Multimedia Content security, Depth Signature Algorithm, Key generation*

I. INTRODUCTION

The creation, preservation, and sharing of image, video, and music data have been made easier by the rapid advancements in digital technology. Cloud computing is an ideal solution for managing this data due to its affordability, scalability, and simplicity. Cloud storage is a popular choice for both businesses and consumers to store and transfer multimedia content across extensive networks. Nevertheless, the risk of data breaches, piracy, unlawful access, and integrity violations is increased by the storage of private multimedia files in the cloud.

Multimedia is more significant to business, more intricate, and larger than text. The transmission and storage of multimedia are essential for digital marketing, education, healthcare, and leisure. Content leakage, financial loss, and reputational damage are all potential consequences of unsecure systems. Research priorities encompass the security, privacy, authenticity, and accessibility of audiovisual content in cloud storage systems. These issues are addressed by contemporary multimedia security solutions.

Distributed, multi-tenant cloud systems are more susceptible to internal and external intrusions. Storage containers, APIs, user passwords, and inadequate encryption may be exploited by attackers. Illegal redistribution is simplified by the act of sharing multimedia assets. Multimedia data in dynamic cloud ecosystems is susceptible to security breaches with the current security solutions. The implementation of DRM, watermarking, encryption, access control, and secure key management is therefore essential for maximum protection.

Multiple levels of multimedia security safeguard against the access, publishing, and transfer of cloud content. Data accuracy and privacy are ensured through the use of AES/RSA encryption and hashing. Digital watermarking is implemented to incorporate multimedia proprietor information. We strongly oppose the act of unauthorized duplication and

DOI: https://doi.org/10.5281/zenodo.20487752

distribution. Cloud users are safeguarded through the implementation of RBAC and multi-factor authentication.

The three components of hybrid security are policy enforcement, encryption, and intelligence monitoring. The security of multimedia that is transferred and stored is guaranteed. Distribution and navigation are simplified through permission-based mechanisms. Robust encryption, secure key management, watermarking, and real-time threat detection are implemented to establish a scalable framework for cloud-based multimedia systems. This comprehensive approach is necessary to ensure the consistent delivery of digital information in a networked environment, maintain user trust, and safeguard intellectual property.

II. BACKGROUND WORK

Multimedia storage in the cloud must be highly secure. Multimedia cloud computing is also known as P2P multimedia computing, content delivery networks, multimedia computing over grids, and server-based computing. It provides infrastructure for high-performance computing (HPC).

Diverse forms of attacks are prevented by numerous fundamental systems. Cloud computing benefits from each of these methodologies. The preponderance of cloud computing is comprised of client-server computing. Outline the three most essential information security protocols.

- A tested Encryption/Decryption.
- Strict Access Mechanism
- A scheduled information backup theme.

On Demand Security Architecture

The Jianyong bird genus' cloud server user data was protected by Principle Wang, Associate in Nursing, Xiaomin Wang, and an on-demand security architecture. Three methods exist for safeguarding cloud computing. The principal domains are storage, services, and networks. This storage cabinet offers adaptability. Furthermore, there is a guarantee of perpetual security that is user-transparent. The user expressed apprehension regarding the cloud's security. How can a client ascertain whether their data would be abused by a blackhat community? Consequently, there are a significant number of security options. Cloud server data is safeguarded, despite the considerable time and expertise required to establish numerous security protocols through the use of a variety of encryption and decryption methods. Upon completion, the aforementioned functions satisfactorily.

Hybrid Encryption Algorithms

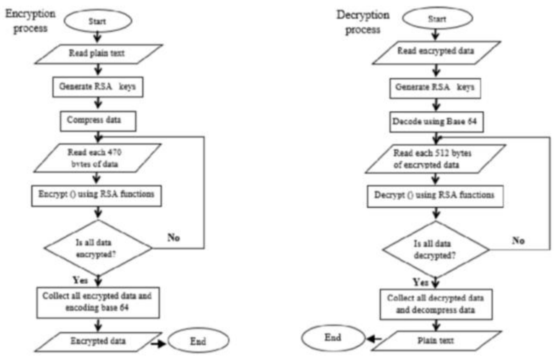

Figure1: RSA Encryption and Decryption Process Flowchart

DOI: https://doi.org/10.5281/zenodo.20487752

implies that cloud computing users are required to submit their login information in plaintext. This algorithm is employed to encrypt passwords. Implementing a hybrid algorithm:

1. Password encryption by using Ceaser Cipher.
2. Repeat algorithm using RSA algorithmic rule.
3. Encrypt the resultant by mono alphabetic substitution methodology.

Developers benefit from anonymous cloud security. This method is preferable to others, despite the fact that font size has an impact on performance. C. Utilizing RSA for Data Security. Parsi Kalpana and Sudha Singaraju implemented RSA to safeguard cloud data. Cloud data security is the primary objective of this investigation. Three phases comprise the methodology:

1. Key Generation
2. Encryption
3. Decryption

The key size is not specified in the document. The performance of approaches is substantially diminished by the size of the keys. The calculation of "e" becomes more challenging as the magnitude of the keys increases. There is no more straightforward approach to determining this figure.

Elliptic Curve Cryptography

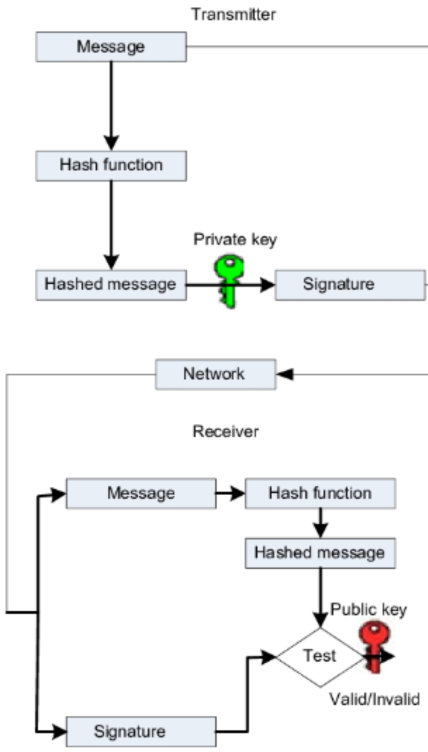

Figure2: Digital Signature Generation and Verification Process

Elliptic curve cryptography is the dominant form of public key cryptography. In the field of digital signatures and cryptography, elliptic curve cryptography was advocated by Veerraju Gampala, Srilakshmi Inuganti, and Satish Muppidi. This technique is employed to encrypt and authenticate cloud data transmission. Digital signature and Diffie-Hellman key exchange methods were improved by elliptic curves.

DOI: https://doi.org/10.5281/zenodo.20487752

Fog Computing for Data Security.

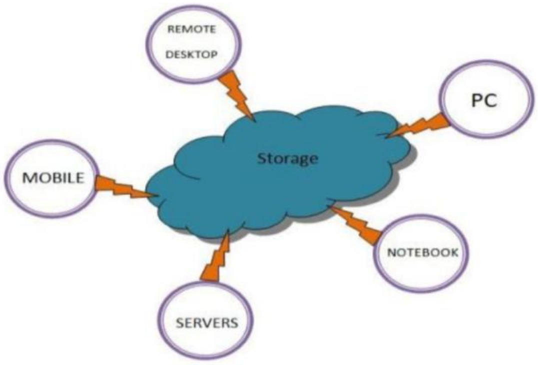

Figure3: Cloud Storage Architecture and Device Connectivity Model

The use of Offensive Decoy Technology to protect data. This method clearly identifies anomalous patterns in the access of cloud storage data. The primary goal is to prevent the misuse of user data. Cloud security is achieved through the utilization of fictitious data by Fog Computing. This method prevents attackers from identifying deceptive assaults and verifying material. Fog computing mitigates Twitter breaches in two distinct ways. Initially, cloud service providers may disseminate inaccurate information. Another approach involves employing fictitious user-generated data on social media profiles. A cloud service that is seldom employed presents false data as genuine. Decoy documents that contain the user's cloud server data will be employed to detect unauthorized access. This investigation examined the unauthorized access to local file system data by masquerades. The method employs decoy and user behavior identification technologies to improve detection, as indicated by research.

III. LITERATURE SURVAY

Kumar, R., and Singh, P. (2025). Cloud storage and controlled dissemination are made easier by AI-driven multimedia security. To prevent multimedia duplication, their strategy makes use of blockchain-based ownership verification, adaptive encryption, and improved threat detection.

Chen, L., and Park, J. (2025). This paper presents a multimedia cloud security framework supported by blockchain technology. Smart contracts prevent IP transfer and piracy by protecting content ownership and access management.

Alshammari, F., and Gupta, S. (2024). A quantum-resistant cloud multimedia encryption system was developed by researchers. To defend massive volumes of multimedia data against quantum assaults, they employ lattice-based encryption and safe key management.

Rodriguez, M., and Iqbal, T. (2024). In this work, multimedia streaming in hybrid cloud systems is protected through the use of attribute-based encryption (ABE). To safeguard copyrighted content, it makes use of decentralized cloud networks, secure streaming, and adaptive access management.

Patel, D., and Verma, A. (2023). An intrusion detection method for multimedia cloud storage based on deep learning is presented. Their system improves security by detecting abnormal access patterns and preventing the acquisition of dangerous content.

DOI: https://doi.org/10.5281/zenodo.20487752

Hassan, M., and Lee, K. (2023). This paper offers a multimedia protection architecture for cloud distribution systems that is centered on DRM. The system uses licensing, encryption, and watermarks to safeguard intellectual property.

Nguyen, T., and Sharma, V. (2022). The authors suggest a straightforward encryption method for sending multimedia data between cloud and peripheral computing. Their approach lowers the computational overhead of multimedia transmission while maintaining security.

Garcia, E., and Mehta, R. (2022). In order to protect encrypted multimedia data in cloud computing and storage, this study employs homomorphic encryption.

Omar, N., and Banerjee, S. (2021). Decentralized access control for multimedia material across cloud systems is defined by researchers. Data transfer, robustness, and integrity are all enhanced by distributed authentication.

Kim, H., and Rao, P. (2021). This study protects cloud-stored audiovisual content with symmetric encryption and robust digital watermarking. It stops redistribution and safeguards ownership.

Ali, Z., and Chatterjee, K. (2020). CP-ABE, or ciphertext-policy attribute-based encryption, is used for cloud storage and multimedia sharing. For authorized users, their method guarantees precise access control and content protection.

Thompson, J., and Rao, S. (2020). Identity-based encryption is advised by this study for cloud multimedia storage. The technology preserves confidentiality, integrity, and access control while improving distributed multimedia key management.

IV. RESULTS

Cloud-stored content is safeguarded by this innovative approach. This approach safeguards video formats. We ensure the security of multimedia assets on a variety of cloud platforms.

Numerous multimedia formats and software applications are not compatible with the system. A distinctive video signature approach. Stereo depth signatures are generated without the necessity for depth signal analysis, which necessitates substantial computational resources. Multimedia content administration is simplified by the dual-layer system. This investigation investigates the preservation of multimedia assets through content-based copy detection (CBCD). Get the signatures of the source entity using this function. Ibpage enquiry components are constructed by signers.

The potential object's similarity to the original is subsequently assessed for duplication.

Images for the project:

Figure4.1: Cloud connection

DOI: https://doi.org/10.5281/zenodo.20487752

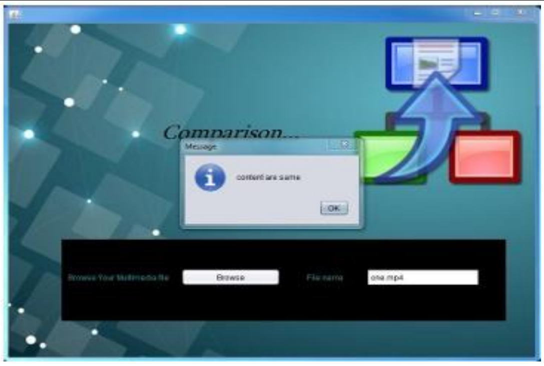

Figure4.2: Content matching

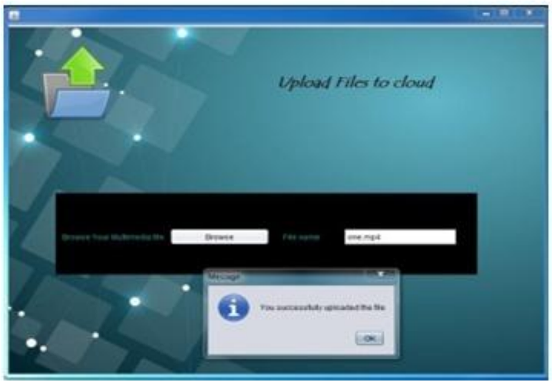

Figure4.3: Successfully upload content

V. CONCLUSION

This study safeguards multimedia data by implementing a secure multimedia security architecture for cloud storage and delivery. Multimedia content is safeguarded from intrusions through the implementation of sophisticated encryption, key management, digital watermarking, authentication, and access control. Decentralized storage and encrypted transmission enhance data privacy. Enhances scalability and efficacy. It guarantees content ownership and facilitates cloud distribution. It is capable of supporting high-performance processing, CDNs, and multimedia transmission. This research establishes a secure architecture for cloud-based multimedia distribution and storage systems, thereby enhancing trust.

REFERENCES

1. P. Cano, E. Batle, T. Kalker, and J. Haitsma, “A review of algorithms for audio fingerprinting,” in Proc. IEEE Workshop Multimedia Signal Process., Dec. 2002, pp. 169–173.
2. J. Dean and S. Ghemawat, “MapReduce: Simplified data processing on large clusters,” in Proc. Symp. Oper. Syst. Design Implementation (OSDI’04), San Francisco, CA, USA, Dec. 2004, pp. 137–150
3. J. Deng, W. Dong, R. Socher, L. Li, K. Li, and L. Fei-Fei, “Imagenet: A large-scale hierarchical image database,” in Proc. IEEE Conf. Comput. Vis. Pattern Recog. (CVPR’09), Miami, FL, USA, Jun. 2009, pp. 248–255. [

DOI: https://doi.org/10.5281/zenodo.20487752

4. A. Hampapur, K. Hyun, and R. Bolle, “Comparison of sequence matching techniques for video copy detection,” in Proc. SPIE Conf. Storage Retrieval Media Databases (SPIE’02), San Jose, CA, USA, Jan. 2002, pp. 194–201.
5. S. Ioffe, “Full-length video fingerprinting. Google Inc.,” U.S. Patent 8229219, Jul. 24, 2012.
6. A. Kahng, J. Lach, W. Mangione-Smith, S. Mantik, I. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe, “Watermarking tech- niques for intellectual property protection,” in Proc. 35th Annu. De- sign Autom. Conf. (DAC’98), San Francisco, CA, USA, Jun. 1998, pp. 776 781.
7. N. Khodabakhshi and M. Hefeeda, “Spider: A system for f inding 3D video copies,” in ACM Trans. Multimedia Comput., Commun., Appl. (TOMM), Feb. 2013, vol. 9, no. 1, pp. 7:1–7:20.
8. S. Lee and C. Yoo, “Robust video fingerprinting for content based video identification,” IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 7, pp. 983–988, Jul. 2008.
9. H. Liao, J. Han, and J. Fang, “Multi-dimensional index on hadoop distributed file system,” in Proc. IEEE Conf. Netw., Archit. Storage (NAS’10), Macau, China, Jul. 2010, pp. 240–249.
10. Z. Liu, T. Liu, D. Gibbon, and B. Shahraray, “Effective, and scalable video copy detection,” in Proc. ACM Conf. Multimedia Inf. Retrieval (MIR’10), Philadelphia, PA, USA, Mar. 2010, pp. 119–128.

DOI: https://doi.org/10.5281/zenodo.20487752