© SEP 2025 | IRE Journals | Volume 9 Issue 3 | ISSN: 2456-8880
DOI: doi.org/10.64388/IREV9I3-1710526-059

# Video Content Verification System

KUCHANNAGARI SATHWIKA[1], K. BALAKRISHNA MARUTHIRAM[2]
[1]*MCA Scholar, Department of Information Technology, University College of Engineering, Science & Technology Hyderabad Jawaharlal Nehru Technological University Hyderabad Kukatpally, Hyderabad, Telangana, India.*
[2] *Assistant Professor of CSE, Department of Information Technology, University College of Engineering, Science & Technology Hyderabad, Jawaharlal Nehru Technological University Hyderabad, Kukatpally, Hyderabad, Telangana, India.*

***Abstract- The primary objective of this project is to design a framework that fosters collaboration between humans and intelligent systems to guarantee the secure delivery of trusted video content across Social Media Networks (SMNs). The framework is built upon three core principles: User Trust Assignment – Each user is allocated a trust score based on their past behaviour and activity history. Intelligent Content Agent – A decision-making agent determines whether content should be automatically published, flagged for human review, or rejected. Video Integrity Verification – Continuous monitoring ensures the authenticity and integrity of video files throughout the streaming process. By integrating these mechanisms, the framework enhances the overall trustworthiness of SMNs while also contributing to optimized capital expenditure and resource utilization.***

## I. INTRODUCTION

The exponential growth of the Internet has led to the emergence of numerous web applications and social multimedia network (SMNs) such as Instagram, X, and Chrome, which have revolutionized the way people communicate and interact worldwide. These platforms have simplified the exchange of information, enabling users to share ideas, opinions, and multimedia content seamlessly. At the same time, they have opened new opportunities for businesses and organizations to connect with wider audiences and directly engage with customers across the globe. Alongside social networking platforms, video-sharing services like YouTube, Dailymotion, and Vimeo have further expanded online interaction by supporting the distribution of text, images, and videos among millions of users.

I.

III.

The advancement of distributed systems and Internet technologies has also driven the popularity of video-on-demand (VOD) and live streaming services that often operate on peer-to-peer (P2P) networks. These systems are now deeply embedded in SMNs, enabling applications in video conferencing, online learning (MOOCs), e-health, e-teaching, and remote collaboration. With millions of participants worldwide, such services encourage massive content generation and interaction. However, the rapid growth of user-generated content has created challenges related to security, trust, and content management. The continuous flow of data often overloads networks, introduces vulnerabilities, and makes it difficult for service providers to regulate and analyze the authenticity of shared information. Therefore, building trustworthy SMNs—where data reliability, authenticity, and security are assured—has become a critical concern.

By integrating these features, the framework aspires to minimize resource consumption while fostering a safer and more reliable multimedia ecosystem. Ultimately, this approach contributes to enhancing the securities, authenticity, and credibility of social multimedia networks, created a more dependable space for the users and content creators.

## II. LITERATURE REVIEW

Gao et al. – A popularity-driven video discovery scheme for the centralized P2P-VoD system Gao and colleagues propose an innovative approach to accelerate video discovery in centralized Peer-to-Peer Video-on-Demand (P2P-VoD) environments. The approach adopts a storage model driven by popularity, organizing videos in a binary tree

© SEP 2025 | IRE Journals | Volume 9 Issue 3 | ISSN: 2456-8880
DOI: doi.org/10.64388/IREV9I3-1710526-059

hierarchy based on their ranking in popularity. Experimental results validate that this mechanism not only minimizes video discovery delays but also optimizes system resource utilization, making content retrieval more efficient.

Taleb and Taleb explore user experience enhancement within social networks by designing a system for personalized multimedia content channels. Their method enables automatic scheduling and playback management based on user preferences, thereby improving accessibility and convenience for social media users. However, while this system improves content customization and delivery, it does not address the critical issue of securing video content against malicious or unauthorized uploads.

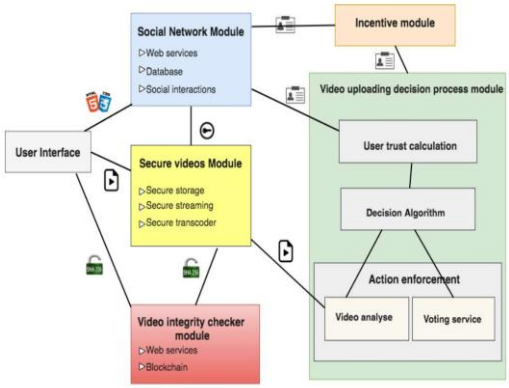
Liang, Lin, and She focus on improving a reliability of service evaluations mobile social networks. They introduce two mechanisms, bTSE and SrTSE, which are specifically designed to resist review-based attacks that threaten service credibility. Their work contributes to strengthening trust and authenticity in service-oriented mobile environments. Nevertheless, their study primarily addresses service evaluation rather than video content authenticity, leaving a gap in tackling content-specific security concerns.

## III. MATERIALS AND METHODS

The proposed system introduces a generalized framework for trustworthy social media networks (smns) by ensuring secure and reliable delivery of video content.

Key features:
Includes trust calculations, voting, incentives, secure video delivery, and integrity verification module.
Leverages user history and collaborative behavior to ensure accurate trust assessment.
Adapts video players functionalities and introduces a video uploading decision process to maintain quality and authenticity of content.

System Architecture:




The dataset undergoes preprocessing and augmentation, followed by classification (using DL models) and detection (using YOLO). Models are evaluated with standard metrics to ensure accuracy.

a) Dataset
Stores trusted and untrusted video data for training and testing.

b) User module:
Multiple users can register and authenticate themselves by logging in.
After successful login, users can upload text posts (tweets) or videos to share with others and the admin.
The content may include both violent and non-violent material.
Once done, users can log out to securely terminate their session.

c) Admin module:
The admin logs in with credentials for privileged access.
Admin can view all user-uploaded tweets and videos.
By selecting videos, the system predicts and classifies violent content such as fighting or murder.
If harmful content is detected, the admin can remove it from the platform to protect users.
Importantly, deletions are invisible to users, ensuring they are not exposed to unsafe material.

c) Algorithms

- VGG19 (Convolutional Neural Network)

A deep learning model with 19 layers, pre-trained on ImageNet dataset. Used for feature extraction and classification of video frames. In this project, VGG19 is applied to classify videos into violent/untrusted or non-violent/trusted categories. Advantage → High accuracy in image/video classification.

© SEP 2025 | IRE Journals | Volume 9 Issue 3 | ISSN: 2456-8880
DOI: doi.org/10.64388/IREV9I3-1710526-059

- Image Data Augmentation

Used to increase dataset variety and avoid overfitting. Techniques applied: rescaling, flipping, zooming, rotating. Helps the model generalize better to new/unseen videos.

- Adam Optimizer

Optimization algorithm for training deep learning models. Automatically adjusts learning rate for faster and more efficient convergence. Advantage → Reduces training time and improves stability.

- Categorical Crossentropy

Loss function used for multi-class classification. Measures the difference between predicted output and actual labels. Guides the model to improve accuracy during training.

- Early Stopping (Callback Function)

Training automatically stops when loss ≤ 0.05 or when no improvement is seen.Prevents overfitting and saves computational resources.

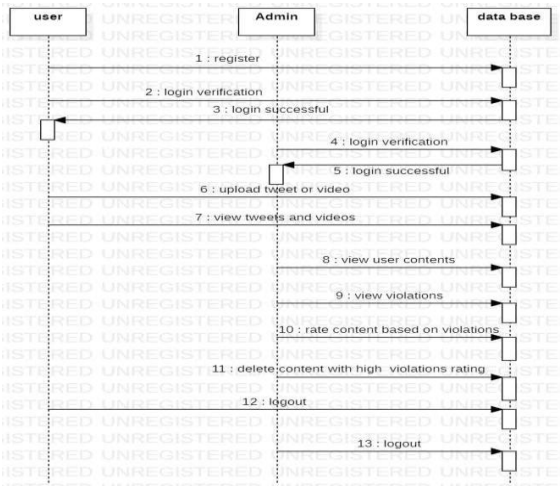
## IV. SYSTEM IMPLEMENTATION

System implementation involves converting the planned system into a working one. It includes technical analysis, operational studies, and the application of methods and tools for effective functioning. The key objective is to ensure smooth input, processing, and output of data while maintaining accuracy and reliability.

Use Case Diagram:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

Sequence Diagram




A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

a). Logical Design

The logical design represents the abstract view of the system, describing data flow, inputs, and outputs without focusing on physical aspects. It is mostly expressed through models and diagrams, such that entity-relationship (er) diagrams, to depict the structure and relationship of data.

b). Physical Design

The physical design specifies how the system will actually operate. It defines how data was entered, validates, processed, stored, and displayed. Physical design generally covers 3 areas:

- User interface design – define how user interact with the system (data entry, navigation, display of information).
- Data design – specify how data is structured and stored.
- Process design – explains how data flow through the system, including validations, transformations, and security.

c) Input Design

Input design serves as the connecting link between the end user and the system. It involves

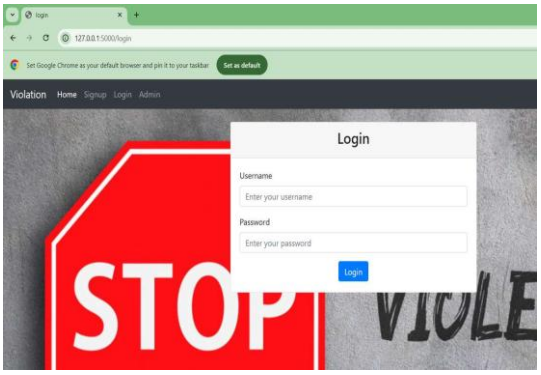
© SEP 2025 | IRE Journals | Volume 9 Issue 3 | ISSN: 2456-8880
DOI: doi.org/10.64388/IREV9I3-1710526-059

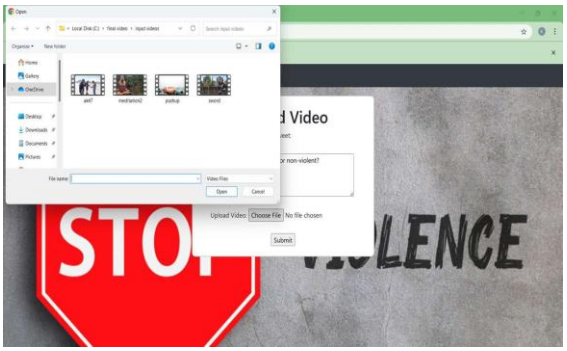
creating clear specifications and methods to organize data before it is processed. Data can be obtained either through manual entry by users or by capturing information from physical documents

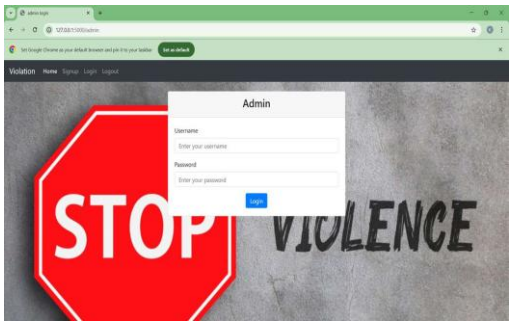
d) Output Design

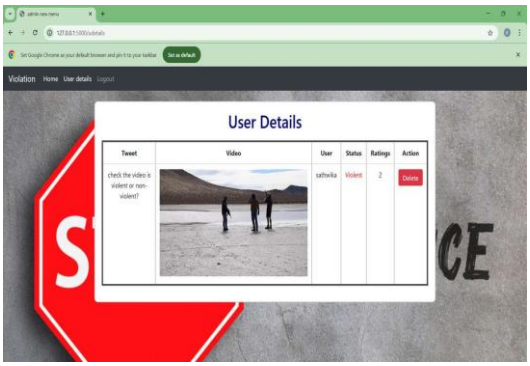
Output is the final result of processing, which must meet user requirements and be presented clearly. Outputs may be displayed on screen or generated as hard copies. Well-structured output enhances decision-making and user satisfaction.

## V. SCREENSHOTS


## CONCLUSION

This study has introduced a comprehensive framework designed to strengthen the security and reliability of Social Multimedia Networks (SMNs), with a focus on the safe delivery of video content. The rapid growth of SMNs has transformed global communication by enabling effortless interaction and sharing among users. However, such connectivity also raises major concerns regarding trust, data security, and content integrity.

To tackle these challenges, the proposed framework integrates human judgment and machine intelligence to ensure that only trusted video content is shared within the network. A key element of this approach is the concept of user trust, determined through historical behavior, collaboration, and activity patterns. By assigning trust levels and utilizing reputation mechanisms, the framework fosters a digital environment built on authenticity, transparency, and security.

The system architecture incorporates several modules, including trust evaluation, voting, incentive mechanisms, secure video delivery, and integrity verification. Together, these modules enhance

decision-making, content moderation, and quality assurance while reducing the spread of unverified or malicious content. Additional features, such as adaptive video players and upload decision modules, further reinforce security while optimizing resource utilization.

Beyond safeguarding content, the framework also promotes cost-effectiveness and efficiency by minimizing unnecessary resource consumption during content analysis. As a result, it not only secures SMNs but also contributes to a more sustainable infrastructure.

Ultimately, this work lays the foundation for building a trustworthy SMN ecosystem where users can confidently share and consume content without fear of security breaches. While the framework marks an important step forward, ongoing research and real-world implementation will be essential to fully realize its potential in creating safe, reliable, and user-centric digital environments.

Future Scope: The system can be extended to other crops and diseases using diverse datasets, IoT-enabled drones, and mobile imaging for large-scale monitoring. Enhancements such as multilingual, farmer-friendly interfaces, and advanced models like Vision Transformers with continual learning will further improve accuracy, adaptability, and accessibility for intelligent, automated crop disease management.

REFERENCES

[1] Gao, et al. (2016). *A Popularity-Driven Video Discovery Scheme for the Centralized P2P-VoD System.* IEEE Transactions on Multimedia.

[2] G. Wu, Z. Liu, L. Yao, J. Deng, and J. Wang, *"A Trust Routing for Multimedia Social Networks,"* The Computer Journal, vol. 58, no. 4, pp. 688–699, Apr. 2015. This paper introduces a fuzzy-based trust model embedding both social trust and QoS metrics to improve routing in multimedia social networks.

[3] Z. Wang, *"Data-driven Approaches for Social Video Distribution,"* arXiv, Jun. 2015. This work presents frameworks for distributing video content via social networks by integrating data-driven insights from social propagation behaviors.

[4] Z. Wang, *"Secure Delivery Method for Preserving Data Integrity of a Video Frame with Sensitive Objects,"* Applied Sciences, 2023. Focuses on frame-level integrity, using logging, hashing, and signature-based verification to secure video content.

[5] Y. Sun, H. Cao, W. Qi, and J. Zhang, *"Improving the security and quality of real-time multimedia transmission in cyber-physical-social systems,"* J. Information Processing Systems, 2018. Addresses real-time video streaming in IoT-like networks using sliding-window retransmission and token-based tampering detection.

[6] E. Liu, Z. Liu, F. Shao, and Z. Zhang, *"A Game-Theoretical Approach to Multimedia Social Networks Security,"* Scientific World Journal, vol. 2014, Article ID 791690, 2014. Proposes a Nash-equilibrium-based trust-access control model in multimedia social networks.

[7] L. Masinde and K. Graffi, *"Peer-to-Peer based Social Networks: A Comprehensive Survey," arXiv preprint*, Jan. 2020. Discusses decentralized, privacy-centered P2P social networks as trust-aware alternatives to centralized platforms.

[8] E. G. Virdi and N. S. Talwandi, *"Visual Truth in the Digital Age: A Review of Image and Video Authentication and Verification Approaches,"* J. Advanced Research in Computer Graphics and Multimedia Technology, 2021. Reviews multimedia forensics and video integrity verification—essential for combating fake or tampered content.

[9] Media forensics on social media platforms: a survey, EURASIP Journal on Information Security, 2021. Surveys multimedia source identification and forgery detection techniques especially tailored to social media contexts.

[10] M. Kosslyn and others, *"Interpersonal Trust within Social Media Applications: A Conceptual Literature Review,"* IntechOpen, 2020–2022. Discusses how multimodal content (e.g. video,

voice) impacts trust in social media, including the challenges posed by deepfakes.

[11] E. Sun, R. Escriva, M. K. Goldberg, M. Hayvanovych, M. Magdon-Ismail, B. K. Szymanski, W. A. Wallace, and G. T. Williams, *"Measuring behavioral trust in social networks,"* in Proc. IEEE ISI, 2010. Investigates behavioral trust metrics that can be adapted for video-sharing platforms.

[12] CyVOD: a novel trinity multimedia social network scheme, Multimedia Tools and Applications, vol. 76, no. 18, 2016. Proposes a DRM-aware multimedia social network framework balancing content protection and usability.

[13] Thabit, *"Trust management and data protection for online social networks,"* IET Communications, 2022. Introduces group-key cryptography and differential privacy methods for enhancing trust and data protection in social networks.

[14] Named Data Networking security model, *"Named Data Networking,"* Wikipedia, 2025. Describes data-centric trust where each data packet is cryptographically signed, enabling integrity and provenance verification—a model that could inspire your framework.