

# Review of Computer Engineering Research

2025 Vol. 12, No. 3, pp. 107-119

ISSN(e): 2410-9142

ISSN(p): 2412-4281

DOI: 10.18488/76.v12i3.4284

© 2025 Consientia Beam. All Rights Reserved.




## Cloud-based video systems: A review of security threats and solutions

 **Prasad A Hatwalne<sup>1+</sup>**

 **Abhishek Dhore<sup>2</sup>**

 **Rinku Badgujar<sup>3</sup>**

 **Manoj Brahme<sup>4</sup>**

 **Minal A. Pardey<sup>5</sup>**

<sup>1</sup>*Teshwantrao Chavan College of Engineering, Nagpur, India.*

Email: [hatwalneprasad1@gmail.com](mailto:hatwalneprasad1@gmail.com)

<sup>2</sup>*Department of CSE, MITSOC, MIT ADT University, Pune, India.*

Email: [abhishekdhore811@gmail.com](mailto:abhishekdhore811@gmail.com)

<sup>3</sup>*Department of Computer Science and Engineering, School of Computing, MIT Art Design and Technology University Pune, India.*

Email: [rinku.badgujar@gmail.com](mailto:rinku.badgujar@gmail.com)

<sup>4</sup>*Department of Information Technology, St. Vincent Pallotti College of Engineering and Technology, Nagpur, India.*

Email: [hodit@stvincentngp.edu.in](mailto:hodit@stvincentngp.edu.in)

<sup>5</sup>*Department of Computer Engineering, P. R. Pote Patil College of Engg & Management, Amravati, India.*

Email: [minalpardey@gmail.com](mailto:minalpardey@gmail.com)



(+ Corresponding author)

## ABSTRACT

### Article History

Received: 21 March 2025

Revised: 27 May 2025

Accepted: 20 June 2025

Published: 8 July 2025

### Keywords

Access control  
Cloud security  
Data encryption  
Intrusion detection  
Privacy preservation  
Video frameworks.

With the rapid growth of cloud computing, along with the recent development of video-based applications and social platforms, there is a need for cloud-based video frameworks. These frameworks employ scalable and economical methods for processing, storing, and delivering video content. The shift to the cloud for video services introduces many security concerns that can compromise the integrity, confidentiality, and availability of the video data they handle. Data breaches, unauthorized access, distributed denial of service (DDoS) attacks, vulnerabilities in encryption, and access control mechanisms are the main security challenges faced by cloud-based video frameworks, which this paper thoroughly reviews. This paper explores the challenges and discusses how they can affect both service providers and end users. The review also highlights state-of-the-art solutions presented in the literature and best practices to mitigate these threats. Some prominent solutions include encryption techniques, access control models, intrusion detection systems, and privacy-preserving algorithms. Additionally, the document addresses how advanced technologies like AI and blockchain can be used to enhance the security of cloud-based video services. This review compiles recent research and industry practices, providing a comprehensive overview of the current security posture and effective strategies for constructing a more secure cloud-based video framework in the future.

**Contribution/Originality:** This article examines the problems and explains how they may affect both service providers and end consumers. This analysis integrates recent research and industry practices to provide an in-depth review of the current security posture and viable strategies for building a more secure cloud-based video framework in the future.

## 1. INTRODUCTION

Video services in the pandemic era have been significantly impacted by the advancement of cloud computing, which has transformed the way digital content is distributed and consumed. Modern multimedia applications rely heavily on cloud-based video frameworks for streaming, storage, and processing in a scalable, efficient, and cost-effective manner. These frameworks have been applied across various domains, including entertainment, education,

healthcare, and communication, demonstrating unparalleled flexibility and accessibility for users [1]. However, in addition to streamlining operations, migrating from traditional on-premises video infrastructure to cloud solutions presents some security challenges that must be addressed to protect sensitive video content and ensure the trustworthiness of the service [2].

With the increasing use of cloud computing, the vulnerability of data and services to potentially malicious actors in a cloud environment is also increasing, making cloud security a primary focus. Maintaining proper security in the cloud computing environment is essential to ensure the confidentiality, integrity, and availability of data, as well as compliance with regulatory requirements. As more organizations adopt cloud-native video solutions to reduce costs and increase flexibility, video content, user data, and the integrity of streaming services have become key targets for malicious actors. Service provider and user information are at risk, including unauthorized logins, unauthorized data modifications, DDoS attacks, content leakage, and other threats [3].

The advantages of cloud infrastructure, including elasticity and cost-effectiveness, have enabled service providers to process large-scale video data and serve high-quality video to multiple devices. While these benefits are numerous, the nature of the cloud environment—with its inherent complexity and level of openness—can make it vulnerable to a range of security threats. Due to the complexity of cyber-attacks, there is a demand for security in cloud-based video frameworks.

To constantly adapt to the rapidly changing landscape of cloud environments, which includes the proliferation of services and new technologies, there is a great need for security that is dynamic and extensible [4].

Since security is a vital concern of the implemented cloud-based video frameworks, this paper presents an overview of the security threats these frameworks face in the cloud and the state-of-the-art solutions to mitigate such risks. By studying the existing security situation and current and emerging methods, this survey aims to provide an informative view of how to design a more secure cloud video infrastructure, thereby contributing to the development of secure and reliable multimedia in the cloud [5, 6].

This paper presents a comprehensive review of the security challenges associated with cloud-based video frameworks, focusing on key issues such as data breaches, unauthorized access, DDoS attacks, and vulnerabilities in encryption and access control mechanisms.

The major contributions of this paper include:

- We conduct systematic identification and analysis of principal security threats involved in cloud-based video frameworks and detail their effects on service providers and end-users.
- This article aims to perform a comprehensive review of available and proposed security solutions and techniques to address these issues, such as new encryption methods, secure access, and intrusion detection systems.
- We discuss how emerging technologies such as AI and blockchain can enhance the security of cloud video ecosystems.
- This paper presents a comprehensive overview of the key components of a cloud-based video service's threat landscape and actionable outcomes that the industry should consider when developing and deploying more secure services by synthesizing academic literature, use cases from the industry, and current research.

The remainder of this paper is organized as follows: In Section 2, we present the background on cloud-based video frameworks, their architecture, and security threats. Section 3 explores the security challenges in cloud-based video frameworks.

Section 4 reviews state-of-the-art security solutions, highlighting both well-established techniques and cutting-edge innovations. Emerging technologies such as AI and Blockchain are discussed in Section 5 for building a secure cloud-based video framework. Section 6 summarizes the key contributions of this paper and outlines potential avenues for future research on this important topic.

## 2. CLOUD-BASED VIDEO FRAMEWORKS ARCHITECTURE AND INHERENT SECURITY CHALLENGES

### 2.1. Cloud-Based Video Frameworks Architecture

Cloud-based video frameworks are designed to leverage the scalability and flexibility of the cloud to deliver video content to users on various device types and locations. These frameworks typically include the following key components in their architecture:

- Video ingestion and encoding: This part handles capturing video input from different sources, such as live cameras or uploaded files, and encoding it for streaming. The encoded video is then uploaded to the cloud for further processing [7].
- Content Delivery Network (CDN): CDNs form an essential component of cloud-based video structures that utilize CDN technology to distribute video files to points of presence on a network of servers that are more geographically distributed, thereby minimizing latency and supporting the streaming of higher-quality video content [8].
- Video Storage: The resulting video content is securely stored using cloud storage systems. We have these storage systems for managing large amounts of data, with built-in redundancy to ensure information availability in case of failure [4].
- Streaming Server: The streaming server delivers video to the end user. It handles user requests, adjusts video quality based on network conditions (adaptive bitrate streaming), and ensures a seamless playback experience.
- User Authentication and Access Control: This section manages user authentication to ensure that only authorized users can access specific video content. It also enforces access control policies to prevent unauthorized viewing of video content.
- Monitoring and Analytics: Most video solutions have monitoring tools and analytics to track user engagement, video performance, and system health. Analytics are used to ensure content is delivered to users in the right format at the right time.

### 2.2. Inherent Security Challenges

Although there are many advantages to cloud-based video frameworks, the architecture presents a number of security challenges that must be addressed to ensure the protection of video content, user data, and the integrity of the entire system. Several inherent security challenges include:

- Data Confidentiality: Video content stored in the cloud and transmitted through it is susceptible to unauthorized access and eavesdropping. To ensure data confidentiality, video content used for AI purposes should be encrypted during storage and transmission to prevent misuse by malicious entities [4].
- Data integrity: Video content must be provisioned to prevent tampering and corruption, thereby ensuring the integrity of the content. This is particularly critical for live streaming services, as any modification may affect the content delivered to viewers [9].
- Unauthorized Access and Identity Management: Ensuring that specific video content reaches only authorized users is a significant challenge. Insecure authentication mechanisms and inadequate access controls can lead to unauthorized access, content theft, and privacy violations [10].
- DDoS Attacks: Cloud-based video frameworks can be targeted with DDoS attacks, where malicious actors attempt to overload the streaming server or CDN by continuously bombarding it with multiple requests, resulting in service outages and degraded performance [11].
- Content piracy is a major concern for content providers, as it involves protecting video content from unauthorized downloading, sharing, or streaming. Intellectual property (IP) rights are essential for producing

films or TV series; however, breaches related to IP can lead to significant revenue loss and legal challenges [12].

- Scalability and Resource Management: With the increasing number of people consuming video-based content, cloud-based video frameworks should be updated to handle scalability effectively. A key challenge is to ensure that security mechanisms, such as encryption, access control, and monitoring, do not adversely affect performance or scalability [13].
- Compliance with regulations: When the frameworks used to segment cloud-based video handle sensitive user information, they must adhere to various data protection laws; in Europe, the General Data Protection Regulation (GDPR), and in the United States, the Health Insurance Portability and Accountability Act (HIPAA). Compliance, coupled with operational agility, will require strong security measures [14].

Such security threats further emphasize the need for robust security features in cloud video platforms. By addressing these challenges, service providers can secure video content, safeguard user data, and maintain customer confidence in a highly competitive environment.

### 3. SPECIFIC SECURITY CHALLENGES IN CLOUD-BASED VIDEO FRAMEWORKS

While cloud video frameworks are powerful within an organization and offer unique advantages in scalability, flexibility, and cost-effectiveness, they are also vulnerable to several security issues. The primary areas of cybersecurity challenges include data breaches, unauthorized access, DDoS attacks, and encryption vulnerabilities. These categories highlight the critical threats that must be mitigated to protect both the video content and the system as a whole.

#### 3.1. Data Breaches

One of the most critical security dangers of cloud-based video storage is information breaches. Sensitive video content and user data are stored and processed remotely in a cloud environment, often in various geographic locations and data centers. Such distribution increases the risk of data access by unauthorized individuals, either through external infiltration or from insiders within an organization [15]. Video content is sensitive in nature and can expose proprietary media content, end-user data, and other sensitive information over data breaches. As a result, service providers suffer considerable financial damage, legal liabilities, and reputational harm. Exploitation of security vulnerabilities can be due to factors such as vulnerabilities in cloud storage systems and inadequate access control limitations. Fortunately, data breaches can be prevented with strong encryption, strict access control policies, system audits, and compliance with data protection laws.

#### 3.2. Unauthorized Access

This may occur due to credential compromise, insecure authentication mechanisms, or insufficient access control policies [16]. Hacking into unauthorized data can cause data leakages, content piracy, and unauthorized video content distribution. It can also be used by attackers to manipulate or erase important data, leading to service disruptions. Password reuse, lack of multi-factor authentication (MFA), and misconfigured access control lists (ACLs) are common issues. Implementing effective validation methods (e.g., MFA, RBAC, continuous access logs monitoring) can help prevent unauthorized access.

#### 3.3. DDoS Attacks

Cloud-based video frameworks are significantly susceptible to DDoS attacks. Attackers in a DDoS attack try to overload the video service infrastructure by sending excessive traffic, degrading performance or completely knocking out the service [11]. DDoS attacks render services unavailable, leading to a poor user experience and loss of revenue, as well as potentially damaging the service provider's reputation. These DDoS attacks are typically carried out

through botnets, where a number of compromised devices generate traffic to the targeted service. DDoS Attack Protection: To defend against DDoS attacks, service providers can utilize cloud-based DDoS protection services, implement traffic filtering and rate limiting, and design their architecture to be resilient and scalable.

### 3.4. Encryption Vulnerabilities

Attacks on encryption pose a significant threat to the confidentiality and integrity of video data in cloud infrastructures. Although encryption is commonly used to protect data in transit or at rest, vulnerabilities in the encryption algorithms or their implementation can make them attractive targets for potential attackers [4]. Video content is often encrypted by security protocols such as Data Encryption Standard (DES), AES, Double DES (MSG), and Advanced Encryption Standard. The most common issues are outdated or weak encryption algorithms, incorrect key management, and implementation mistakes. These threats can only be countered by using strong, up-to-date encryption standards, secure key management processes, and regular assessments of encryption standard implementation.

## 4. REVIEW WORK

Table 1 summarizes details regarding various advanced techniques and methodologies discussed in the literature that can improve Security in different domains, including image secret sharing, cloud-based security frameworks, cooperative cloud security, etc. Various systems have been introduced in terms of security enhancement that guarantee the protection and integrity of data during storage and communication in different stages. Reference Yan et al. [17] proposed a new multiparty verification approach for image secret sharing, which improves the security and reliability of the shared images by allowing multiple parties to verify the correctness of the shared image without revealing the actual content. This is important to ensure that the secrets remain protected and that the image does not change.

A novel encryption technique for medical images that combines visual encryption, image watermarking, and band amplification and extraction technology was proposed in Priya and Santhi [18]. This method embeds authentication watermarks in encrypted medical images, thereby enhancing the secure transmission of sensitive medical data and ensuring its authenticity during transmission.

In Rathore et al. [19], the use of blockchain technology for IoT networks was studied, and a block-based architecture has been proposed. This blockchain-based security architecture aims to decentralize security mechanisms to maintain data integrity and prevent unauthorized access. This feature in integrated solutions is very useful for securing IoT devices and their communication, due to growing security concerns in the IoT environment. Xiong and Luo [20] extended the research to address data searchability and efficient data searchability in cloud storage environments, proposing a searchable encryption scheme for huge datasets. This method signature allows for fairly efficient searching over encrypted data without the need to visit the corresponding tables, thereby securing the data while maintaining the functionality required for large-scale data processing.

Furthermore, a framework combining compressive sensing with encryption was proposed by Manikyam and Devi [21] to enhance image security in cloud environments. This dual-function approach simultaneously compresses and encrypts images, effectively reducing storage requirements while ensuring the secure transmission and storage of data.

Data access control in cloud storage was further improved by Rathod et al. [22], who introduced a role-based access control mechanism that uses data fragmentation to enhance security. This method optimizes storage costs while ensuring that data remains confidential, providing an efficient and secure solution for cloud storage.

Privacy-preserving collaborative computations were advanced by Li and Christensen [23], who introduced an asynchronous averaging algorithm using Shamir's Secret Sharing. This algorithm enables distributed

participants to compute averages without revealing their individual data, making it particularly useful in privacy-sensitive scenarios.

Security challenges in IoT-based Wireless Sensor Networks (WSNs) were addressed by VenkataRao and Ananth [24], who integrated a hybrid optimization algorithm with Shamir's Secret Sharing to ensure secure data transmission and enhance network performance. This framework effectively tackles the security issues prevalent in IoT environments.

In vehicular ad hoc networks (VANETs), a lightweight authentication scheme using elliptic curve cryptography was proposed by Alshudukhi et al. [25]. This scheme ensures privacy preservation and efficient authentication, which is crucial for the high-mobility environment of VANETs.

An innovative approach to image encryption was introduced by Panigrahy et al. [26], utilizing artificial neural networks to enhance the speed and robustness of the encryption process. This method also improves the Structural Similarity Index (SSIM), making it suitable for various applications requiring efficient and secure image encryption.

Authentication protocols leveraging Physical Unclonable Functions (PUFs) and Shamir's Secret Sharing were presented by Chen et al. [27]. These protocols provide robust authentication for IoT devices, ensuring data integrity and protection against unauthorized access.

The unique security challenges of cloud-based Electronic Health Record (EHR) systems were addressed by Ganiga et al. [28], who proposed a security framework ensuring data confidentiality, integrity, and availability, tailored specifically for managing EHRs in cloud environments.

For secure transmission in e-healthcare systems, particularly for intraoral gingivitis images, Sarkar et al. [29] introduced a neural soft computing approach. This method combines neural networks with soft computing techniques to ensure secure and efficient transmission, enhancing patient data protection in e-healthcare.

A distributed remote e-voting system leveraging Shamir's Secret Sharing Scheme was presented by Tejedor-Romero et al. [30]. This system ensures voter privacy and data integrity by distributing voting data among multiple parties, making it a secure solution for remote electronic voting. Deep neural networks were employed by Alarood et al. [31] in developing a secure transmission method for medical images in e-health applications. This approach focuses on ensuring the confidentiality and integrity of medical images during transmission, utilizing advanced encryption techniques.

In the field of steganography, Onuma and Miyata [32] introduced a context-aware steganography method based on Shamir's Secret Sharing Scheme and mapping within the DCT domain. Steganography enables secure and covert communication, and embedding secret shares into DCT coefficients is a common method used to achieve this. Jia et al. [33] combined homomorphic encryption with chunk-based convolutional neural networks to propose a privacy-preserving image classification algorithm. This method allows computations to be performed on encrypted datasets, making it particularly suitable for securing cloud-based image classification processes.

Velmurugan et al. [34] designed a selective data sharing scheme in which cloud-based decentralized trust management was incorporated, offering a secure and decentralized approach to trust management and data privacy in cloud settings.

Orthogonal compressive sensing with optimizations was used in an image encryption method in Wen et al. [35], guaranteeing good-quality reconstruction while maintaining the security of encryption. K-Means clustering, MD5, and AES-256 encryption are among the methods used for secure image transmission and storage of images.

A comparative study on secret sharing methods was conducted by Voudouris et al. [36], evaluating the efficiency and security of Lagrange interpolation versus Newton interpolation in distributed key sharing. This study provides insights into best practices for secret sharing in distributed systems. Finally, Abdel Hakeem and Kim [37] introduced a centralized threshold key generation protocol mixing Shamir's Secret Sharing with HMAC authentication. Such a protocol ensures that a key can be generated and managed securely, providing a comprehensive solution for centralized systems. The GSCSO-IHNN model, as described in Ramachandran et al. [38], aims to enhance cloud-



based security by integrating genetic and sine-cosine optimization with improved hierarchical neural networks. The proposed model performs cyber threat detection and mitigation in cloud computing.

**Table 1.** Comparative analysis of literature review.

Reference no	Methodology	Key findings	Limitations
Yan, et al. [17]	Multiparty verification in image secret sharing using cryptographic protocols	Enhanced security and reliability in image secret sharing with multiparty verification.	Complex implementation and computational overhead.
Priya and Santhi [18]	Visual medical image encryption with watermarking	Ensures secure transmission and authentication of medical images	Potential degradation of image quality due to watermarking
Rathore, et al. [19]	Blockchain-based decentralized security for IoT networks	Provides robust security and data integrity for IoT networks	Scalability issues and high resource consumption
Xiong and Luo [20]	Searchable encryption for large datasets in cloud	Efficient searching of encrypted data without compromising security	High computational cost for large datasets
Manikyam and Devi [21]	Image security in cloud with compression and encryption using compressive sensing	Simultaneous compression and encryption reduce storage and enhance security	Potential loss of data quality due to compression
Rathod, et al. [22]	Role-based secure data access control using data fragmentation	Enhanced data confidentiality and optimized storage costs	Complex data management and potential performance overhead
Li and Christensen [23]	Privacy-preserving asynchronous averaging using Shamir's Secret Sharing	Allows secure collaborative computations without revealing individual data	Complexity in implementation and synchronization issues
VenkataRao and Ananth [24]	Hybrid optimization and Shamir secret sharing for IoT-based WSN	Secure data transmission and enhanced network performance	Integration complexity and potential latency
Alshudukhi, et al. [25]	Lightweight authentication with privacy-preserving scheme for VANETs using elliptic curve cryptography	Efficient and secure authentication for high-mobility VANETs	Limited by the computational capabilities of VANET devices
Panigrahy, et al. [26]	Artificial neural network-based image encryption with improved SSIM	High-speed and robust image encryption with enhanced SSIM	Requires significant computational resources
Chen, et al. [27]	Strong-PUF-based authentication protocols leveraging Shamir's secret sharing.	Robust IoT device authentication and data integrity	Complex protocol design and potential implementation challenges
Ganiga, et al. [28]	Security framework for cloud-based EHR system	Ensures the confidentiality, integrity, and availability of EHR data	Implementation complexity and compliance with healthcare regulations
Sarkar, et al. [29]	Neural soft computing for secure transmission of intraoral gingivitis images	Secure and efficient transmission of medical images	High computational complexity
Tejedor-Romero, et al. [30]	Distributed remote e-voting system using Shamir's secret sharing	Secure and private remote e-voting	Potential scalability and synchronization issues
Alarood, et al. [31]	Secure medical image transmission using deep neural networks	Confidential and intact transmission of medical images	High computational requirements
Onuma and Miyata [32]	Correlation-based steganography using Shamir's Secret Sharing and DCT domain	Covert and secure communication	Complex embedding and extraction processes
Jia, et al. [33]	Privacy-preserving image classification using homomorphic encryption and chunk-based CNN	Secure and efficient image classification in the cloud	High computational overhead

Reference no	Methodology	Key findings	Limitations
Velmurugan, et al. [34]	Data selective sharing with decentralized trust management	Provably secure data sharing with trust management	Implementation complexity and potential trust issues
Wen, et al. [35]	Image encryption using optimized orthogonal compressive sensing	High-quality image reconstruction and secure encryption	Potential quality loss and computational cost
Abdel Hakeem and Kim [37]	Secret sharing a key in a distributed way: Lagrange vs Newton	Comparison of two secret sharing methods for distributed key sharing	Differences in efficiency and security
Abdel Hakeem and Kim [37]	Centralized threshold key generation with Shamir's Secret Sharing and HMAC	Secure key generation and management	Centralization risks and potential single point of failure
Ramachandran, et al. [38]	Cyber-threat detection using the GSCSO-IHNN model	Efficient cyber-threat detection in cloud environments	Model complexity and resource requirements

## 5. ROLE OF ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN TECHNOLOGIES IN ENHANCING THE SECURITY OF CLOUD-BASED VIDEO FRAMEWORKS

The integration of Artificial Intelligence (AI) and blockchain technologies into cloud-based video frameworks presents significant opportunities for enhancing security. Both technologies offer unique capabilities that address various security challenges associated with cloud environments, such as data breaches, unauthorized access, and maintaining the integrity of video content. Below, we discuss the potential benefits and challenges of incorporating AI and blockchain into these frameworks.

### 5.1. Role of AI in Enhancing Security

#### 5.1.1. AI-Driven Threat Detection and Response

- **Benefits:** AI algorithms, especially machine learning (ML) algorithms, can be implemented to monitor the vast amount of data generated by cloud-based video frameworks in near real-time. Learning these algorithms can help discover patterns and detect anomalies to predict potential security threats such as unauthorized access attempts or DDoS attacks. Being AI-powered, security systems can respond to threats automatically by sending alerts, blocking suspicious activities, or isolating targeted network segments. This proactive approach enables you to prevent and minimize the impact of security incidents more effectively.
- **Challenges:** The implementation of AI systems is one of the major challenges. Training these AI models also requires access to a significant amount of computational power and data. Furthermore, AI-based security tools must evolve constantly to keep pace with changing threats, which can be resource-intensive. There is a possibility of a false positive, where actual activity that poses no threat could trigger a flag, potentially affecting service.

#### 5.1.2. AI-Enhanced Encryption and Authentication

- **Benefits:** AI can be used to create more secure encryption algorithms and authentication methods. There are specific examples, such as AI-powered systems that can dynamically change the encryption level based on the information's sensitivity or relevant threat level. Additionally, AI can enhance biometric authentication systems, such as those based on facial or voice recognition, making it more difficult for unauthorized users to access sensitive video data.
- **Challenges:** Implementing secure and user-friendly AI-enhanced encryption and authentication methods appears to be the key challenge. It is difficult to achieve that balance, particularly when operating in the cloud where latency and performance are critical. Moreover, adversarial attacks can also be launched against AI systems, where attackers input manipulated data to mislead the AI models.



## 5.2. Role of Blockchain in Enhancing Security

### 5.2.1. Decentralized Security and Data Integrity

- **Benefits:** Blockchain technology offers a decentralized way of securing data that is, by design, resistant to tampering. For cloud-based video frameworks, blockchain can be implemented to generate an indelible ledger of all transactions and interactions that occur with video content. It makes it so that if someone tries to change the contents or logs of a node, they would have to change at least half of the nodes to avoid detection, as there are multiple copies all over the blockchain network. Blockchain also adds transparency to it all, as the integrity of the data can be verified by all stakeholders.
- **Challenges:** Blockchain is known for its secure nature, but the consensus mechanisms needed to verify transactions can result in performance overheads. In real-time applications such as live streaming, this is a significant issue, as these mechanisms can delay video content processing and delivery [27]. The scalability of blockchain networks is also a challenge, as the size of the blockchain increases, requiring more storage and computational resources over time.

### 5.2.2. Smart Contracts for Automated Security Policies

- **Benefits:** Cloud-based video frameworks can implement security policies automatically through self-executed contracts because smart contracts are agreements embedded directly within code. For example, smart contracts can facilitate access control by allowing only users with the appropriate permissions to view or edit video content. Additionally, they can be used to track licensing and royalties to ensure creators are paid promptly, and content is distributed based on predetermined criteria.
- **Challenges:** Developing and maintaining smart contracts is a complex issue. Since the contracts are immutable, any security vulnerabilities caused by bugs in smart contract code become difficult to fix after deployment. Moreover, the legal framework surrounding smart contracts is still in its infancy, and businesses may grapple with questions regarding their validity in various legal jurisdictions.

## 5.3. Potential Synergies and Combined Benefits

When combined, AI and blockchain technologies can offer synergistic advantages for augmenting the security of cloud-based video architectures.

- **Enhanced Trust and Accountability:** AI can be employed to sift through blockchain data and identify patterns associated with fraudulent activity or breaches, thereby adding an extra layer of security. Conversely, blockchain can serve as a transparent and unchangeable ledger of AI decisions, addressing the need for trust in AI-powered security systems by providing verifiable audit trails.
- **Scalable and Adaptive Security Solutions:** By predicting network load and controlling consensus mechanisms accordingly, AI can optimize the functioning of the blockchain, significantly improving its scalability and performance. Additionally, blockchain facilitates the secure distribution of AI models and updates across a decentralized network, ensuring that all nodes in a distributed system use the latest and most secure versions of AI algorithms.

## 5.4. Challenges in Integration

While these synergies can yield benefits, there are many challenges that will exist with the convergence of AI and blockchain in cloud-based video systems:

- **Interoperability:** One of the major challenges is ensuring that AI and blockchain systems can seamlessly interact with one another and existing cloud infrastructure. This is necessary to build standardized protocols and interfaces to allow seamless integration.

- **Resource Requirements:** AI and blockchain both require a significant amount of resources, including processing power, storage, and bandwidth. Integrating them into cloud-based video frameworks adds latency, potentially increases costs, and may even necessitate changes to the underlying infrastructure.
- **Regulatory and Ethical Considerations:** The application of AI and blockchain for cloud video frameworks should also adhere to certain legal and ethical frameworks, specifically those relating to data privacy and AI decision-making laws. In addition, compliance with regulations may vary from one jurisdiction to another, so companies should carefully consider this before deciding.

## 6. CONCLUSION AND FUTURE WORK

The potential security threats in cloud-based video systems have been discussed in this paper, and the possible uses of emerging technologies such as AI and blockchain in improving security in this area have also been explored. We are at a point where the need to have secure mechanisms for secure video content, data integrity, and trust is critical for users as cloud-based video frameworks are being adopted by many industries. They identified numerous major security flaws with cloud video frameworks, including data breaches, unauthorized access, DDoS attacks, and encryption vulnerabilities. These and other challenges pose severe threats to the confidentiality, integrity, and availability of video content and end-user data. At the core of all these issues is the use of AI techniques, specifically machine learning, which are driving significant innovations in the security of cloud systems. AI-powered protection of networks against attackers includes real-time defense against various security threats using AI-driven threat detection, adaptive encryption, and differential authentication mechanisms. However, deploying AI is not trivial; considerations such as resource requirements, false positives, and regular updates for new attacks must be taken into account. Blockchain provides tamper-resistant data securing through decentralized mechanisms resistant to unauthorized changes. The immutable logs associated with blockchain and smart contracts that automate security policies can make cloud-based video frameworks more transparent and reliable. Nonetheless, challenges such as scalability, performance overheads, and complexity in smart contract development need to be addressed. The joint implementation of AI and blockchain technologies in cloud-based video framework security can produce synergistic effects. AI can enhance the efficiency of blockchain operations, and blockchain can offer AI a way to create verifiable audit trails for decisions made by algorithmic systems, resulting in a stronger, more agile security solution. Future work should focus on developing more scalable solutions that integrate cloud, video, and IT technologies such as AI and blockchain.

These features include improved resource utilization, better interoperability, and ensuring that the integrated system can grow with the demand placed by modern cloud environments. Shift your attention to developing AI models capable of predicting and preventing emerging security threats before they become catastrophic in scale. This might involve the use of advanced machine-learning algorithms, such as deep learning and reinforcement learning, to enhance the ability to detect and respond to incursions. As there are many questions around the scalability of using blockchain technology in a cloud-based video architecture, performance issues remain as concerns. Therefore, we advocate for future work in pursuing novel consensus schemes (proof-of-stake or sharding) to further reduce latency and securely increase throughput in blockchain networks. Nonetheless, we should ensure this kind of utilization complies with ethical and agency requirements, as these are inseparable aspects of video-based platforms, especially in standards for a future cloud-based environment alongside techniques like AI and blockchain technology. This research respects that, and the development of frameworks guiding the ethical use of these technologies—particularly regarding data privacy and user consent—will need to be a consistent concern. Lastly, future research should involve real-world case studies and implementation trials to validate these AI and blockchain technologies by contributing more advanced security solutions. These include studies that assess deployment-related barriers such as cost, user adoption, or impact on service performance, to better inform applications in the industry.

**Funding:** This study received no specific financial support.

**Institutional Review Board Statement:** Not applicable.

**Transparency:** The authors state that the manuscript is honest, truthful, and transparent, that no key aspects of the investigation have been omitted, and that any differences from the study as planned have been clarified. This study followed all writing ethics.

**Competing Interests:** The authors declare that they have no competing interests.

**Authors' Contributions:** All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.

## REFERENCES

- [1] N. Gruschka, L. L. Iacono, and M. Jensen, "Cloud security—The security impact of cloud computing," *IEEE Security & Privacy*, vol. 10, no. 2, pp. 62–65, 2012. <https://doi.org/10.1109/MSP.2012.56>
- [2] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," *The Journal of Supercomputing*, vol. 63, pp. 561–592, 2013. <https://doi.org/10.1007/s11227-012-0831-5>
- [3] M. A. Shah and A. Ahmed, "The security of cloud-based video streaming frameworks: A survey," *IEEE Access*, vol. 8, pp. 144517–144528, 2020. <https://doi.org/10.1109/ACCESS.2020.3015561>
- [4] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 843–859, 2012. <https://doi.org/10.1109/SURV.2012.060912.00182>
- [5] A. Kaloxylou, "Security in cloud computing: Issues and current solutions," *Future Generation Computer Systems*, vol. 32, pp. 449–456, 2014. <https://doi.org/10.1016/j.future.2013.07.009>
- [6] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications*, vol. 79, pp. 88–115, 2017. <https://doi.org/10.1016/j.jnca.2016.11.027>
- [7] D. Jiang, F. Wen, M. Liu, and T. Zhao, "A cloud-based architecture for online video streaming services," *International Journal of Cloud Computing and Services Science*, vol. 2, no. 4, pp. 307–317, 2013. <https://doi.org/10.11591/closer.v2i4.1455>
- [8] M. Pathan, J. Broberg, and R. Buyya, "Maximizing CDN performance: Architectures and techniques," *International Journal of Computer Applications in Technology*, vol. 31, no. 4, pp. 321–329, 2008. <https://doi.org/10.1504/IJCAT.2008.020588>
- [9] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *2012 International Conference on Computer Science and Electronics Engineering*, 2012, vol. 1: IEEE, pp. 647–651.
- [10] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *Journal of Internet Services and Applications*, vol. 1, pp. 7–18, 2010. <https://doi.org/10.1007/s13174-010-0007-6>
- [11] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: Methods, systems and tools," *Ieee Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 303–336, 2013. <https://doi.org/10.1109/SURV.2013.052213.00046>
- [12] S. Akramullah, "Content protection for cloud-based media services: Challenges and solutions," *IEEE Consumer Electronics Magazine*, vol. 3, no. 3, pp. 68–73, 2014. <https://doi.org/10.1109/MCE.2014.2307936>
- [13] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities," in *2008 10th IEEE International Conference on High Performance Computing and Communications*, 2008: Ieee, pp. 5–13.
- [14] S. Pearson, *Privacy, security and trust in cloud computing*. In *Privacy and Security for Cloud Computing*. Springer. [https://doi.org/10.1007/978-1-4471-4189-1\\_1](https://doi.org/10.1007/978-1-4471-4189-1_1), 2013.
- [15] X. Liu, "Data breaches in cloud computing: Analysis, mitigation, and prevention," *IEEE Access*, vol. 8, pp. 182434–182446, 2020. <https://doi.org/10.1109/ACCESS.2020.3025639>
- [16] J. Cheng and R. Adams, "Unauthorized access in cloud services: Trends, challenges, and future directions," *IEEE Security & Privacy*, vol. 18, no. 4, pp. 26–35, 2020. <https://doi.org/10.1109/MSEC.2020.2994667>

- [17] X. Yan, J. Li, Z. Pan, X. Zhong, and G. Yang, "Multiparty verification in image secret sharing," *Information Sciences*, vol. 562, pp. 475-490, 2021. <https://doi.org/10.1016/j.ins.2021.03.029>
- [18] S. Priya and B. Santhi, "A novel visual medical image encryption for secure transmission of authenticated watermarked medical images," *Mobile Networks and Applications*, vol. 26, no. 6, pp. 2501-2508, 2021. <https://doi.org/10.1007/s11036-019-01213-x>
- [19] S. Rathore, B. W. Kwon, and J. H. Park, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network," *Journal of Network and Computer Applications*, vol. 143, pp. 167-177, 2019. <https://doi.org/10.1016/j.jnca.2019.06.019>
- [20] Y. Xiong and M. X. Luo, "Searchable encryption scheme for large data sets in cloud storage environment," *Radioengineering*, vol. 33, no. 2, p. 223, 2024. <https://doi.org/10.13164/re.2024.0223>
- [21] N. R. H. Manikyam and M. S. Devi, "A framework for leveraging image security in cloud with simultaneous compression and encryption using compressive sensing," *Rev. d'Intelligence Artif.*, vol. 35, no. 1, pp. 85-91, 2021. <https://doi.org/10.18280/ria.350110>
- [22] S. G. Rathod, M. D. Salunke, H. B. Jadhav, D. A. Ajalkar, D. B. Satre, and D. Bonde, "Role Based Secure Data Access Control for Cost Optimized Cloud Storage Using Data Fragmentation While Maintaining Data Confidentiality," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 7s, p. 316, 2023. <https://doi.org/10.17762/ijritcc.v11i7s.7005>
- [23] Q. Li and M. G. Christensen, "A privacy-preserving asynchronous averaging algorithm based on shamir's secret sharing," in *2019 27th European Signal Processing Conference (EUSIPCO)*, 2019: IEEE, pp. 1-5.
- [24] S. VenkataRao and V. Ananth, "A hybrid optimization algorithm and Shamir secret sharing based secure data transmission for IoT based WSN," *International Journal of Intelligent Engineering & Systems*, vol. 14, no. 6, p. 498, 2021. <https://doi.org/10.22266/ijies2021.1231.44>
- [25] J. S. Alshudukhi, Z. G. Al-Mekhlafi, and B. A. Mohammed, "A lightweight authentication with privacy-preserving scheme for vehicular ad hoc networks based on elliptic curve cryptography," *IEEE Access*, vol. 9, pp. 15633-15642, 2021. <https://doi.org/10.1109/ACCESS.2021.3053043>
- [26] A. K. Panigrahy *et al.*, "A faster and robust artificial neural network based image encryption technique with improved SSIM," *IEEE Access*, vol. 12, pp. 10818-10833, 2024. <https://doi.org/10.1109/ACCESS.2024.3353294>
- [27] S. Chen, B. Li, Z. Chen, Y. Zhang, C. Wang, and C. Tao, "Novel strong-PUF-based authentication protocols leveraging Shamir's secret sharing," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14408-14425, 2021. <https://doi.org/10.1109/JIOT.2021.3065836>
- [28] R. Ganiga, R. M. Pai, and R. K. Sinha, "Security framework for cloud based electronic health record (EHR) system," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, p. 455, 2020. <https://doi.org/10.11591/ijece.v10i1.pp455-466>
- [29] A. Sarkar, J. Dey, M. Chatterjee, A. Bhowmik, and S. Karforma, "Neural soft computing based secured transmission of intraoral gingivitis image in e-health care," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 14, no. 1, pp. 178-184, 2019. <https://doi.org/10.11591/ijeecs.v14.i1.pp178-184>
- [30] M. Tejedor-Romero, D. Orden, I. Marsa-Maestre, J. Junquera-Sanchez, and J. M. Gimenez-Guzman, "Distributed remote e-voting system based on Shamir's secret sharing scheme," *Electronics*, vol. 10, no. 24, p. 3075, 2021. <https://doi.org/10.3390/electronics10243075>
- [31] A. A. Alarood, M. Faheem, M. A. Al-Khasawneh, A. I. Alzahrani, and A. A. Alshdadi, "Secure medical image transmission using deep neural network in e-health applications," *Healthcare Technology Letters*, vol. 10, no. 4, pp. 87-98, 2023. <https://doi.org/10.1049/htl2.12049>
- [32] K. Onuma and S. Miyata, "A proposal for correlation-based steganography using Shamir's secret sharing scheme and DCT domain," in *2021 International Conference on Information Networking (ICOIN)*, 2021: IEEE, pp. 255-260.

- [33] H. Jia *et al.*, "Efficient and privacy-preserving image classification using homomorphic encryption and chunk-based convolutional neural network," *Journal of Cloud Computing*, vol. 12, no. 1, p. 175, 2023. <https://doi.org/10.1186/s13677-023-00537-0>
- [34] S. Velmurugan, M. Prakash, S. Neelakandan, and A. Radhakrishnan, "Provably secure data selective sharing scheme with cloud-based decentralized trust management systems," *Journal of Cloud Computing*, vol. 13, no. 1, p. 86, 2024. <https://doi.org/10.1186/s13677-024-00634-8>
- [35] H. Wen *et al.*, "Exploiting high-quality reconstruction image encryption strategy by optimized orthogonal compressive sensing," *Scientific Reports*, vol. 14, no. 1, p. 8805, 2024. <https://doi.org/10.1038/s41598-024-59277-z>
- [36] A. Voudouris, I. Politis, and C. Xenakis, "Secret sharing a key in a distributed way, Lagrange vs Newton," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1-7.
- [37] S. A. Abdel Hakeem and H. Kim, "Centralized threshold key generation protocol based on Shamir secret sharing and HMAC authentication," *Sensors*, vol. 22, no. 1, p. 331, 2022. <https://doi.org/10.3390/s22010331>
- [38] D. Ramachandran, M. Albathan, A. Hussain, and Q. Abbas, "Enhancing cloud-based security: A novel approach for efficient cyber-threat detection using GSCSO-IHNN model," *Systems*, vol. 11, no. 10, p. 518, 2023. <https://doi.org/10.3390/systems11100518>

*Views and opinions expressed in this article are the views and opinions of the author(s). Review of Computer Engineering Research shall not be responsible or answerable for any loss, damage or liability etc. caused in relation to/arising out of the use of the content.*