Received: 2026-03-04
Accepted: 2026-06-15
Published Online: 2026-06-25
DOI: 10.70454/JRIST.020203

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

Review of Cloud-Based Public Security Video Investigation Systems: Architecture, Challenges, and Future Directions

Sonia Chourasiya*[1], Dr. Pharindra Kumar Sharma[2]

[1]M.Tech Student, Dept. of CSE, SRCEM.
2Associate Professor, Dept. of CSE, SRCEM
*Corresponding Author.: chourasiyasonia24@gmail.com

Abstract

Cloud computing has significantly transformed the way people investigate security video images by enhancing the analytical ability of surveillance technology, scaling and efficiency. Ordinary video surveillance systems have limitations in storage, real-time processing, and analysis of data, cloud computing addresses these issues quite satisfactorily. This paper explores different types of cloud computing models, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), and its applications in public security video studies. The concept of cloud-based video surveillance systems is mentioned along with the methods of data collection, cloud storage solutions, real-time processing, and analytics powered by artificial intelligence. The paper highlights the key benefits of cloud-based security systems which include improved scalability, cost efficiency, real-time monitoring, and AI-based threat detection. To ensure optimal performance, however, issues such as data privacy issues, cyber attacks, interoperability issues and dependency on constant internet connectivity need to be addressed. The paper also examines Indian case studies that have conducted cloud-based video analysis in the law enforcement system and smart city monitoring programs.By implementing the recently emerging technologies such as artificial intelligence, 5G, and edge computing, cloud-based public security systems can enhance the capability to prevent and respond to crimes. The essay discusses the future that should occur and highlights that regulatory frameworks, moral implementation of AI, and superior cloud protection measures are required.

Keywords: Cloud Computing, Video Surveillance, AI-driven analytics, Cybersecurity Threats and Real-time Processing

1. Introduction

Police have been revolutionized by cloud computing as it has been integrated into the monitoring of the police. Problem management and storage space conventions can impair the capabilities of typical monitoring equipment. Traditional systems use most of the local storage facilities, such as real servers or mechanical drives, which are expensive to operate and are likely to lose, or damage, data. These systems too are struggling to keep pace with the sheer and ever-growing volume of footage that contemporary surveillance systems such as air drones, body cameras, or CCTV networks generate. Cloud computing takes care of these issues by offering storage and processing options that can be extended, modified and be inexpensive. The police departments can store numerous photographs and videos in the cloud without the need to acquire equipment on-site.

Received: 2026-03-04
Accepted: 2026-06-15
Published Online: 2026-06-25
DOI: 10.70454/JRIST.020203

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

Security companies can keep huge libraries of surveillance film, which helps with long-term inquiry and legal reviews [1]–[5]. Cloud computing doesn't merely store films; it also makes it easier to look at them. You have to view and check the film by hand when you utilize standard video surveillance. This takes a lot of energy and is easy to mess up. On the other hand, cloud-based systems employ AI and ML to autonomously check videos for faults, recognize faces, and keep track of things in real time. These advanced analytics assist police operations be more accurate and effective by allowing authorities to act quickly when there is a suspected threat.

The cloud also lets people in charge of public safety work collaboratively and obtain information from anywhere. Police, forensic analysts, and security guards at various sites can all see video in real time and look at it. This helps you work out how to deal with problems like crime, terrorist threats, or emergency plans. Cloud solutions also have robust data encryption or cybersecurity capabilities that keep private video recordings safe from anyone who shouldn't be able to watch them. There are a lot of positive things about the cloud for computing, but there are also some bad things about using it for video surveillance. When making sure that programs is both moral and useful, you should think about topics like data privacy, latency, and following the rules. For example, it's hard to tell who has the right to access and control data when it's stored in multiple places and on cloud-based infrastructure. This article talks about how cloud-based platforms improve video analysis, help them expand, and enable you leverage strong AI-driven analytics to make decisions right away. It looks into a lot of different cloud computing ideas, how they might be used in security research, the problems they present, and where they can go in the future. This paper seeks to illustrate the impact of cloud computing on public security video investigation systems through a thorough analysis.

2. Related Work

Mohammad 2024 et al. This study investigates how to augment security and privacy in multi-cloud environments by studying encryption techniques and access control systems. Since multiple cloud providers are required, more comprehensive data security plans are required. To overcome the difficulties in security of sensitive information, the study analyses some encryption methods and access control systems. An in-depth review of privacy laws and security models will identify viable solutions to reduce threats and vulnerabilities. The work is also useful in increasing the security and reliability of cloud computing by improving multi-cloud architectures against probable threats. This guarantees integrity of data, privacy, and controlled access of numerous cloud platforms[6].

Akbar 2024 et al. This study comes up with a safe method of deduplication of large-scale cloud storage aiming to address the challenges of identification of duplicate data. Dynamic Principal Coding (DPC) of the Two Threshold Two Divisor (TTTD) approach is more effective in deduplicating data, but remains security conscious. An index-based strategy can help to increase throughput with minimal CPU power consumption and reduced time to execute. The cross-domain authentication is used to secure data when it is provided to cloud services that are partially trusted. Real-world tests indicate that one can enhance the performance of deduplication that incorporates the aspects of the circulation of the chunks, the period of handling them, and the ratio of deduplication. Reducing the time to compute a hash function (772 ms) compared to existing methods reduces the cost of computing as well [7].

Baur 2024 et al. This paper introduces a secure deduplication method for large-scale cloud storage to address challenges associated with the detection of duplicate data. The Two Maximum Threshold for Two Divisor (TTTD) approach with a dynamic Initial Coding (DPC) allows for deduplication much faster while still keeping security in mind. An index-based method can help speed things up by utilizing less CPU power

Received: 2026-03-04
Accepted: 2026-06-15
Published Online: 2026-06-25
DOI: 10.70454/JRIST.020203

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

while consuming less time to run. Cross-domain authentication keeps data safe when it is sent over websites that aren't fully trusted. Real-world tests show that it is feasible to make deduplication more efficient by changing the way chunks are sent, how long it takes to handle them, and the deduplication ratio. If you can do a hash function faster (772 ms), it costs less to do it than it does currently [8].

Akoh 2024 et al .This article discusses the implications of cloud computing on accounting firms, which include data security, scaling, and production. Adoption of the cloud allows companies to be more flexible and conserve money by allowing them to scale up and down depending on the workload requirements. This enhances team work, simplifies routine work, and streamlines operations. Nonetheless, data security remains a colossal issue. You must have financial data protection through strong encryption, authentication, or compliance solutions. The report provides accountants with the information on how to balance the advantages and disadvantages of cloud computing with the issue of security. This paper provides a strategic recommendation to those firms that are gradually moving to cloud-based solutions. It shows the extent to which cloud technology can be utilized to the maximum without compromising the safety and confidentiality of your data[9].

Abba 2024 et al. This study explores the issues surrounding safety and confidentiality during CoT design and implementation. It examines potential risks and identifies major issues which must be corrected. The paper also discusses on privacy concerns, the security regulations already existing at the moment and issues that remain to be answered. This provides recommendations on how the safety base of the related technologies can be improved to secure the data[1].

Table 1 Literature Summary

Author	**Methodology**	**Research gap**	**Findings**
Zhang 2024 [10]	Blockchain-based platform improves security and research by automating social media forensics.	In social forensics, lack of automation, standardizing, and secure procedures.	Blockchain architecture advances data privacy, threat detection, and forensic stability.
Saini 2024 [11]	In cloud sharing, hybrid structure improves resource economy, trust, and privacy.	Current techniques lack effective resource allocation, trust, and integrated privacy.	Improved privacy, confidence, and resource economy combined with great scalability and accuracy.
Yang 2024 [12]	For effective crowd monitoring and anomaly detection, combined YOLOv5, DeepSORT, and KDE.	In surveillance, lack of merged detection, tracking, placement, and anomaly analysis.	Improved crowd surveillance utilizing YOLOv5, DeepSORT following, positioning as well as and anomaly detection.

Received: 2026-03-04
Accepted: 2026-06-15
Published Online: 2026-06-25
DOI: 10.70454/JRIST.020203

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

Wang 2024 [13]	Metaverse security, privacy concerns, issues, and countermeasures survey.	Metaverse lacks scalability, interoperability systems, strong security, and privacy solutions.	Metaverse presents security, privacy, scalability issues; survey investigates future directions and answers.
Li 2024 [14]	VideoChat combines models for causal inference, event location, and spatiotemporal thinking.	Lack of spatiotemporal thinking and causal inference in chat-centric video understanding.	VideoChat improves causal inference in movies, spatiotemporal reasoning, and event localization.

3. Cloud Computing In Public Security Video Investigations

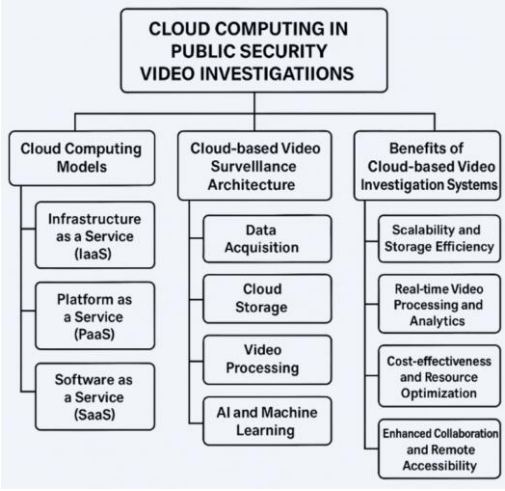

Fig. 1 Cloud Computing in Public Security Video Investigations

A. **Cloud Computing Models:** Cloud computing models provide diverse service levels customized to the needs of security and audio investigation systems.

- **Infrastructure as a Service (IaaS)** gives you simulated computing resources like network access, storage, and CPU on demand, and you only pay for them when you use them. IaaS helps police departments keep and operate a lot of recordings and add more as needed without investing in expensive physical equipment.
- **Platform as a Service (PaaS)** lets developers create, test, and implement apps free from concern for underlying infrastructure. PaaS solutions let law enforcement departments design AI-driven film analysis tools for anomaly detection, facial recognition, and object identification.[15].
- **Software as a Service (SaaS)** offers over-the-internet ready-to-use software applications. Cloud-based video management systems (VMS) and artificial intelligence-powered analytics tools—which enable remote access and agency collaboration—are SaaS platforms for safety video investigation.

Received: 2026-03-04
Accepted: 2026-06-15
Published Online: 2026-06-25
DOI: 10.70454/JRIST.020203

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

B. **Cloud-based Video Surveillance Architecture:** Cloud-based CCTV systems are made of several linked parts that guarantee effective video collecting, processing, and storage.
- **Data acquisition** include gathering video from several sources, including surveillance systems, drones, and cellphones carried by law enforcement personnel [16]–[18].
- **Cloud storage solutions** offer safe storage for superior video material that may grow as needed. Law enforcement can store a lot of data in secured cloud environments, which keeps the data safe and easy to get to.
- **Real-time and batch processing** There are many ways to look at videos. Batch processing lets forensic experts watch recorded video, while real-time processing helps them find suspicious activity right immediately.
- **AI and machine learning for image and video analytics** make it easier to look into things. Algorithms for can watch things, find crimes, and collect useful information from video streams.

C. Benefits of Cloud-based Video Investigation Systems
- **Scalability and Storage Efficiency** Cloud computing allows groups that focus on public safety store a lot of video without having to worry about running out of space. Dynamic increase of storage capacities ensures that agencies can keep surveillance data for lengthy periods of time and get the most out of their money.
- **Real-time Video Processing and Analytics** Cloud-based solutions let you analyze video in real time thanks to artificial intelligence or machine learning. Police can swiftly find prospective threats with automated object detection, identification of faces, or behavior analysis.
- **Cost-effectiveness and Resource Optimization Law** application agencies can reduce the expense in infrastructure that accompanies the traditional methods of observation through cloud resources. Pay-as-you-go pricing plans ensure that resources are utilized in the most optimal manner without wasting money.
- **Enhanced Collaboration and Remote Accessibility** Law enforcement agencies' smooth cooperation with forensic experts is made possible by cloud computing. Safe access to video data from several sites improves reaction times and inter-agency cooperation.[19]–[23].
- **Artificial Intelligence Predictive Security** Predictive analytics using artificial intelligence can be used to identify patterns in crime; machine learning models can be used to predict potential security threats, which is why it can be used to support proactive law enforcement.

4. Challenges and Security Concerns

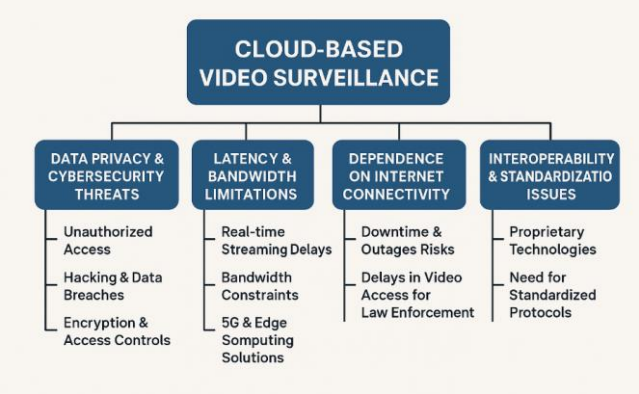

Fig. 2 Cloud Based Video Surveillance

- Data Privacy and Cybersecurity Threats Cloud-based video surveillance stores and processes sensitive data, which is the subject of cyber threats. Unauthorized access, hacking and breach of data may affect

Received: 2026-03-04
Accepted: 2026-06-15
Published Online: 2026-06-25
DOI: 10.70454/JRIST.020203

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

security footage resulting in privacy invasion. Risks should be minimized through encryption, multi-factor authentication and high access controls.

- Latency and Bandwidth Limitations Real-time video streaming and analysis demand high-speed networks and low-latency networks. Video transmission may also be delayed due to bandwidth constraints, which impact the ability to make timely decisions. Latency issues can be minimized with the implementation of 5G and edge computing.
- Legal and Ethical Implications Cloud-based surveillance creates legal and ethical issues over ownership of data, jurisdiction and privacy rights. The responsible implementation is essential in compliance with regional and international regulations, including GDPR.[24]–[27].
- Internet-Connectivity Public security agencies using cloud systems will be susceptible to interruption of internet. Unplanned interruptions or downtime may slow down access to important video footage, affecting law enforcement business.
- Interoperability and Standardization Issues Various cloud vendors operate proprietary technologies, which result in interoperability issues. There is a need to standardize data and system integration among agencies so as to facilitate smooth data exchange.

5. Case Studies and Existing Implementations

With many government and corporate projects using cloud computing for increased monitoring and forensic analysis, India has seen notable developments in cloud-based public security video investigations. Under the Smart Cities Mission, one of the most well-known applications is the smart city surveillance projects whereby artificial intelligence-powered cloud surveillance systems have been installed in Delhi, Mumbai, Hyderabad, and Bengaluru[28]. These initiatives monitor metropolitan areas, control traffic, and improve law enforcement response by combining high-density CCTV cameras, drones, IoT sensors with cloud platforms. For example, the Telangana government has set up a cloud-based Integrated Command and Control Center (ICCC) using artificial intelligence-driven analytics to monitor real-time crime prevention. Another vital application gaining popularity among Indian police agencies is cloud-based forensic video analysis in law enforcement. Cloud-based video analytics solutions help agencies including the Central Bureau of Investigation (CBI), Maharashtra Cyber, and the Delhi Police process and examine digital evidence from surveillance footage. Forensic investigators can use these gadgets to follow movements, make videos clearer, and recognize faces using artificial intelligence algorithms. The National Crime Records Bureau (NCRB) also improved cloud-based crime data storage and video investigation capabilities to help solve cases faster and make investigations more efficient.

Also, people in India are slowly starting to accept AI-powered anomaly detection in public places and important infrastructure. Airports including Delhi's Indira Gandhi International Airport and Mumbai's Chhatrapati Shivaji Maharaj International Airport have deployed cloud-based artificial intelligence surveillance to find illegal entry, unattended luggage, and suspicious activities. For similar hypothetical security issues, financial institutions and corporate security teams are monitoring ATMs, bank branches, and office locations using AI-powered cloud systems. Companies including TCS, Infosys, and Reliance Jio have developed advanced cloud security solutions made for public safety and corporate use. These case studies highlight how cloud computing is transforming public security video investigations carried out in India. Including cloud infrastructure with artificial intelligence and big data analytics would help law enforcement authorities and security specialists ensure real-time situational awareness, boost forensic investigations, and help to prevent crime. Still, problems such data sovereignty rules, cybersecurity threats, and regulatory compliance have to be addressed if India is to guarantee the appropriate and secure implementation of cloud-based surveillance technologies. As technology advances, emerging technologies such blockchain for data security, edge computing enabled by 5G, and AI-driven automation will steadily improve India's public security framework.[29]–[31].

Received: 2026-03-04
Accepted: 2026-06-15
Published Online: 2026-06-25
DOI: 10.70454/JRIST.020203

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

6. Future Directions and Recommendations

As cloud computing continues to evolve, its role in public security video image investigation systems is expected to expand with emerging technologies and innovative solutions. Based on the review of current implementations, the following future directions and recommendations are proposed:

1. **Adoption of Edge Computing and 5G Integration:** To minimize latency and improve real-time video analytics, edge computing is an important technology to integrate with cloud infrastructure. The introduction of 5G networks will additionally enhance the speed at which data is transmitted, thus creating the ability to process high-definition surveillance images more efficiently and with less time.
2. **Enhanced AI and Deep Learning for Video Analytics:** The next generation of public security systems must also take advantage of the advanced AI models, such as deep learning methods, to enhance the accuracy of facial recognition, detecting anomalies, and predictive analytics. Such innovations will enable law enforcement agencies to be proactive in dealing with possible security threats.
3. **Blockchain for Data Security and Integrity:** By using blockchain technology, the security of video footage can be improved by guaranteeing the integrity and traceability of data and making it unalterable. Systems based on blockchains may contribute to an unalterable record of surveillance information to assist in forensic investigations.
4. **Regulatory and Legal Framework Development:** With the growth of cloud-based video surveillance, governments and businesses need to create comprehensive policies to protect privacy, provide ethical guidelines and ensure adherence to national security laws. Consensus standards will provide principles for ethical and legal use of surveillance[32]–[35].
5. **Scalable and Cost-Effective Cloud Solutions:** Research should turn its attention to affordable and scalable cloud storage to help manage the ever-growing amount of video data produced by surveillance. A hybrid cloud approach may be the best solution for public safety agencies.
6. **Interoperability and Standardization:** Creating a common standard for cloud video investigation systems will support data exchange and interoperability among law enforcement departments, security companies and government agencies. Open-source systems and APIs can improve system interoperability.
7. **Ethical AI Implementation and Bias Mitigation:** Ensuring that video analytics powered by AI are unbiased and transparent is quite crucial. Future studies must focus on eliminating bias on recognizing facial features or models of behavior estimation to prevent erroneous profiling and bias[36]–[40].
8. **Citizen Engagement and Public Awareness:** Educating the population on the benefits and drawbacks of cloud-based public safety technologies will increase the chances of people in society gaining trust and collaborating with each other. The involvement of people in the governance of surveillance will be able to influence the policies whereby the requirement of security is counterbalanced with the right to privacy.

By adopting such future orientations, the public security agencies can harness the potential of cloud computing in video investigations and overcome the security, privacy and regulatory compliance challenges. The ongoing development of AI, 5G, blockchain, and hybrid cloud systems will be a key factor in the creation of the new generation of smart and efficient systems to monitor public safety.

7. Conclusion

In the paper at hand, the authors examined how cloud computing can be utilized in investigating public security video images, which is important to note as it has affected surveillance, forensic analysis, and AI-based threat detection. The main goals were to evaluate the benefits, issues and the future of cloud-based security solutions. To do so, the review has discussed the different models of cloud computing, cloud computing architecture, advantages, and case studies with an emphasis on

Received: 2026-03-04
Accepted: 2026-06-15
Published Online: 2026-06-25
DOI: 10.70454/JRIST.020203

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

smart cities, police uses of cloud computing, and AI-based anomaly detection. The research methodology included a comprehensive analysis of the available literature, real-life applications, and technological developments in cloud-based video surveillance. In this analysis, there were important findings that cloud computing can be used to improve the scalability, real-time analytics, and cost efficiency of security systems. Nonetheless, issues like data privacy concerns, interoperability, and cybersecurity threats should be overcome to allow a large scale adoption.This review met its goals by showing how the video investigation process can be enhanced with the help of AI and machine learning integration to use cloud computing. Future studies ought to be on streamlining data protection, regulatory practices, and ethical AI applications. With the assistance of the new technologies such as 5G, edge computing, and sophisticated cloud architectures, the cloud-based security system can move forward and provide even safer and more resilient public security infrastructures.

References

[1] A. A. Abba Ari *et al.*, "Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges," *Appl. Comput. Informatics*, vol. 20, no. 1–2, pp. 119–141, 2024, doi: 10.1016/j.aci.2019.11.005.

[2] J. N. A. M. -, S. P. -, S. V. B. -, and M. D. -, "Enhancing Cloud Compliance: A Machine Learning Approach," *Adv. Int. J. Multidiscip. Res.*, vol. 2, no. 2, pp. 1–16, 2024, doi: 10.62127/aijmr.2024.v02i02.1036.

[3] Y. Wang, M. Zhu, J. Yuan, G. Wang, and H. Zhou, "The intelligent prediction and assessment of financial information risk in the cloud computing model," *Appl. Comput. Eng.*, vol. 64, no. 1, pp. 127–133, 2024, doi: 10.54254/2755-2721/64/20241372.

[4] M. Kaleem, M. A. Mushtaq, and S. K. Hussain, "New Efficient Cryptographic Techniques For Cloud Computing Security," no. June, 2024.

[5] A. Wali and F. Alshehry, "A Survey of Security Challenges in Cloud-Based SCADA Systems," *Computers*, vol. 13, no. 4, 2024, doi: 10.3390/computers13040097.

[6] N. Mohammad, "Multi-Cloud Environments : a Comprehensive Study on Encryption Techniques and Access Control," no. April, 2024.

[7] M. Akbar, I. Ahmad, M. Mirza, M. Ali, and P. Barmavatu, "Enhanced authentication for de-duplication of big data on cloud storage system using machine learning approach," *Cluster Comput.*, vol. 27, no. 3, pp. 3683–3702, 2024, doi: 10.1007/s10586-023-04171-y.

[8] A. Baur, "European Dreams of the Cloud: Imagining Innovation and Political Control," *Geopolitics*, vol. 29, no. 3, pp. 796–820, 2024, doi: 10.1080/14650045.2022.2151902.

[9] Akoh Atadoga, Uchenna Joseph Umoga, Oluwaseun Augustine Lottu, and Enoch Oluwademilade Sodiya, "Evaluating the impact of cloud computing on accounting firms: A review of efficiency, scalability, and data security," *Glob. J. Eng. Technol. Adv.*, vol. 18, no. 2, pp. 065–075, 2024, doi: 10.30574/gjeta.2024.18.2.0027.

[10] A. A. Khan, X. Zhang, F. Hajjej, J. Yang, C. S. Ku, and L. Y. Por, "ASMF: Ambient social media forensics chain of custody with an intelligent digital investigation process using federated learning," *Heliyon*, vol. 10, no. 1, p. e23254, 2024, doi: 10.1016/j.heliyon.2023.e23254.

[11] H. Saini *et al.*, "Hybrid Optimization Machine Learning Framework for Enhancing Trust and Security

Received: 2026-03-04
Accepted: 2026-06-15
Published Online: 2026-06-25
DOI: 10.70454/JRIST.020203

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

in Cloud Network," *IEEE Access*, vol. 12, no. December, pp. 195943–195959, 2024, doi: 10.1109/ACCESS.2024.3520665.

[12] K. Yang and A. Yilmaz, "Crowd Scene Anomaly Detection in Online Videos," *Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci. - ISPRS Arch.*, vol. 48-2–2024, no. June, pp. 443–448, 2024, doi: 10.5194/isprs-archives-XLVIII-2-2024-443-2024.

[13] Y. Wang *et al.*, "A Survey on Metaverse: Fundamentals, Security, and Privacy," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 1, pp. 319–352, 2023, doi: 10.1109/COMST.2022.3202047.

[14] K. Li *et al.*, "VideoChat: Chat-Centric Video Understanding," pp. 1–16, 2023.

[15] Ehsan Bazgir, Ehteshamul Haque, Numair Bin Sharif, and Md. Faysal Ahmed, "Security aspects in IoT based cloud computing," *World J. Adv. Res. Rev.*, vol. 20, no. 3, pp. 540–551, 2023, doi: 10.30574/wjarr.2023.20.3.2481.

[16] S. Zhao, J. Miao, J. Zhao, and N. Naghshbandi, "A comprehensive and systematic review of the banking systems based on pay-as-you-go payment fashion and cloud computing in the pandemic era," *Inf. Syst. E-bus. Manag.*, no. 0123456789, 2023, doi: 10.1007/s10257-022-00617-9.

[17] T. Y. Wu, F. Kong, Q. Meng, S. Kumari, and C. M. Chen, "Rotating behind security: an enhanced authentication protocol for IoT-enabled devices in distributed cloud computing architecture," *Eurasip J. Wirel. Commun. Netw.*, vol. 2023, no. 1, 2023, doi: 10.1186/s13638-023-02245-4.

[18] P. Krishnan, K. Jain, A. Aldweesh, P. Prabu, and R. Buyya, "OpenStackDP: a scalable network security framework for SDN-based OpenStack cloud infrastructure," *J. Cloud Comput.*, vol. 12, no. 1, 2023, doi: 10.1186/s13677-023-00406-w.

[19] M. Suganya and T. Sasipraba, "Stochastic Gradient Descent long short-term memory based secure encryption algorithm for cloud data storage and retrieval in cloud computing environment," *J. Cloud Comput.*, vol. 12, no. 1, 2023, doi: 10.1186/s13677-023-00442-6.

[20] A. R. Al-Ghuwairi, Y. Sharrab, D. Al-Fraihat, M. AlElaimat, A. Alsarhan, and A. Algarni, "Intrusion detection in cloud computing based on time series anomalies utilizing machine learning," *J. Cloud Comput.*, vol. 12, no. 1, 2023, doi: 10.1186/s13677-023-00491-x.

[21] J. Li, W. Xiao, and C. Zhang, "Data security crisis in universities: identification of key factors affecting data breach incidents," *Humanit. Soc. Sci. Commun.*, vol. 10, no. 1, 2023, doi: 10.1057/s41599-023-01757-0.

[22] R. Bhat, N. R. Sunitha, and S. S. Iyengar, "A probabilistic public key encryption switching scheme for secure cloud storage," *Int. J. Inf. Technol.*, vol. 15, no. 2, pp. 675–690, 2023, doi: 10.1007/s41870-022-01084-8.

[23] S. Ahmadi, "Security And Privacy Challenges in Cloud-Based Data Warehousing: A Comprehensive Review," *Int. J. Comput. Sci. Trends Technol.*, vol. 11, pp. 17–27, 2023, [Online]. Available: www.ijcstjournal.org

[24] J. Wang, Y. Liu, S. Rao, R. S. Sherratt, and J. Hu, "Enhancing Security by Using GIFT and ECC Encryption Method in Multi-Tenant Datacenters," *Comput. Mater. Contin.*, vol. 75, no. 2, pp. 3849–3865, 2023, doi: 10.32604/cmc.2023.037150.

[25] S. Stewart Kirubakaran, V. P. Arunachalam, S. Karthik, and S. Kannan, "Towards Developing Privacy-Preserved Data Security Approach (PP-DSA) in Cloud Computing Environment," *Comput. Syst. Sci. Eng.*, vol. 44, no. 3, pp. 1881–1895, 2023, doi: 10.32604/csse.2023.026690.

Received: 2026-03-04
Accepted: 2026-06-15
Published Online: 2026-06-25
DOI: 10.70454/JRIST.020203

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

[26] C. Shekhar Tiwari and V. Kumar Jha, "Enhancing the Cloud Security through RC6 and 3DES Algorithms while Achieving Low-Cost Encryption," *Int. J. Wirel. Microw. Technol.*, vol. 13, no. 5, pp. 48–59, 2023, doi: 10.5815/ijwmt.2023.05.05.

[27] R. R. Irshad *et al.*, "IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Blockchain-Based Approach Toward a Trustworthy Cloud Computing," *IEEE Access*, vol. 11, no. October, pp. 105479–105498, 2023, doi: 10.1109/ACCESS.2023.3318755.

[28] B. Rahul and K. Kuppusamy, "Efficiency Analysis of Cryptographic Algorithms for Image Data Security in Cloud Environment," *IETE J. Res.*, vol. 69, no. 9, pp. 6053–6064, 2023, doi: 10.1080/03772063.2021.1990141.

[29] M. N. Katsantonis, A. Manikas, I. Mavridis, and D. Gritzalis, "Cyber range design framework for cyber security education and training," *Int. J. Inf. Secur.*, vol. 22, no. 4, pp. 1005–1027, 2023, doi: 10.1007/s10207-023-00680-4.

[30] D. K. Murala, S. K. Panda, and S. K. Sahoo, *Securing Electronic Health Record System in Cloud Environment Using Blockchain Technology*, vol. 237, no. February. Springer International Publishing, 2023. doi: 10.1007/978-3-031-22835-3_4.

[31] N. Gaur and S. Singh, "A Behaviour Study on Cloud Eco-System: Data Security Perspective," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 11, no. 6, pp. 172–177, 2023, doi: 10.17762/ijritcc.v11i6.7379.

[32] H. Attou, A. Guezzaz, S. Benkirane, M. Azrour, and Y. Farhaoui, "Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques," *Big Data Min. Anal.*, vol. 6, no. 3, pp. 311–320, 2023, doi: 10.26599/BDMA.2022.9020038.

[33] S. S. Pericherla, "Cloud Computing Threats, Vulnerabilities and Countermeasures: A State-of-the-Art," *ISeCure*, vol. 15, no. 1, pp. 55–112, 2023, doi: 10.22042/isecure.2022.312328.718.

[34] M. Z. Hasan, M. Z. Hussain, Z. Mubarak, A. A. Siddiqui, A. M. Qureshi, and I. Ismail, "Data security and Integrity in Cloud Computing," *2023 Int. Conf. Adv. Technol. ICONAT 2023*, no. April, 2023, doi: 10.1109/ICONAT57137.2023.10080440.

[35] P. Maniatis, "Comparison of Public, Private, Hybrid, and Community Cloud Computing in Terms of Purchasing and Supply Management: A Quantitative Approach," *Int. J. Multidiscip. Res. Anal.*, vol. 06, no. 06, pp. 2359–2369, 2023, doi: 10.47191/ijmra/v6-i6-04.

[36] D. Kumar Sharma, D. Sreenivasa Chakravarthi, A. Ara Shaikh, A. Al Ayub Ahmed, S. Jaiswal, and M. Naved, "The aspect of vast data management problem in healthcare sector and implementation of cloud computing technique," *Mater. Today Proc.*, vol. 80, no. September, pp. 3805–3810, 2023, doi: 10.1016/j.matpr.2021.07.388.

[37] V. V Vegesna, "The Utilization of Information Systems for Supply Chain Management for Multicomponent Productivity Based on Cloud Computing," *Int. J. Manag. Technol. ...*, no. October, 2023, [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4612525%0Ahttps://www.researchgate.net/profile/Vinod-Varma-Vegesna/publication/374949401_The_Utilization_of_Information_Systems_for_Supply_Chain_Management_for_Multicomponent_Productivity_Based_on_Cloud_

[38] V. Varma Vegesna, "A Comprehensive Investigation of Privacy Concerns in the Context of Cloud

Received: 2026-03-04
Accepted: 2026-06-15
Published Online: 2026-06-25
DOI: 10.70454/JRIST.020203

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

Computing Using Self-Service Paradigms," no. October, 2023, [Online]. Available: https://ssrn.com/abstract=4612536

[39] D. Selvaraj, S. M. U. Sankar, D. Dhinakaran, and T. P. Anish, "Outsourced Analysis of Encrypted Graphs in the Cloud with Privacy Protection," *SSRG Int. J. Electr. Electron. Eng.*, vol. 10, no. 1, pp. 53–62, 2023, doi: 10.14445/23488379/IJEEE-V10I1P105.

[40] A. Pakmehr, A. Aßmuth, C. P. Neumann, and G. Pirkl, "Security Challenges for Cloud or Fog Computing-Based AI Applications," pp. 21–29, 2023, [Online]. Available: http://arxiv.org/abs/2310.19459