IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15701

Challenges of Cloud Data Privacy in Surveillance: Legal, Technical, and Ethical Implications

Ahmed S. AlMahmeed

Department of Computer Science, PAAET, Kuwait

Abstract: The migration of surveillance systems to cloud infrastructure has improved scalability and analytics capabilities but introduces distinct privacy challenges: jurisdictional conflicts between GDPR and the CLOUD Act, expanded attack surfaces from third-party integrations, mandatory retention that conflicts with data minimization, and function creep enabled by centralized data lakes. Using case law from Schrems II, breach reports from ENISA, and technical evaluations of federated learning and differential privacy, this paper systematizes core risks of cloud surveillance. We contribute: 1) a taxonomy of seven cloud-surveillance privacy challenges, 2) an end-to-end architecture with privacy controls, 3) a STRIDE+LINDDUN threat model, and 4) a four-layer mitigation framework. Evaluation shows federated learning reduces raw video egress by 98% with 4% F1 loss, while geo-fenced encryption satisfies Schrems II supplementary measures. We argue that technical safeguards alone are insufficient without multilateral legal harmonization and independent oversight.

Index Terms: Cloud surveillance, data privacy, GDPR, CLOUD Act, differential privacy, federated learning, STRIDE, cross-border data, immutability.

I. INTRODUCTION

Video surveillance is undergoing a structural shift from siloed, on-premises DVR/NVR architectures to cloud-native Video Surveillance as a Service (VSaaS) [1]. The driver is scale: cloud storage "scales with your platform" and can ingest "hundreds—or thousands—of new cameras per month", whereas physical servers require costly forklift upgrades [1]. Cloud enables centralized AI for object detection, behavior analysis, and cross-camera tracking.

Yet "cloud computing offers numerous advantages, its inherent reliance on distributed data storage introduces various threats, including unauthorized access, insider attacks, and data leakage" [2]. Surveillance data is inherently sensitive: video of public spaces, biometric identifiers, and metadata like location/time. When this data is "sharded or split up and simultaneously stored in different data centers", legal and technical control fragments [3].

This paper addresses three research questions critical to JCC readership: RQ1: What unique privacy risks emerge when surveillance data moves to multi-tenant, multi-jurisdictional clouds? RQ2: How do existing legal frameworks (GDPR, CLOUD Act, Schrems II) interact with technical safeguards? RQ3: Which privacy-preserving computation techniques are viable for cloud surveillance at scale?

II. BACKGROUND AND RELATED WORK

A. Cloud Surveillance Architecture

Cloud VSaaS stores encrypted video in object storage with metadata indexing. Unlike traditional CCTV, cloud systems enable: 1) Remote access, 2) AI inference pipelines, 3) Elastic retention [1]. Designing storage that ensures "fast, reliable access… is critical, but challenging" [1].

B. Legal Landscape

GDPR mandates data minimization, purpose limitation, and right to be forgotten [4]. Surveillance firms must comply "even if the data has been obtained from outside of the EU" [5]. Schrems II (2020) invalidated Privacy Shield because U.S. surveillance laws create "gaps in the data protection commitments" [6], forcing cloud-dependent operators to implement SCCs + supplementary measures [5].

The U.S. CLOUD Act extends SCA to "data held overseas" and authorizes bilateral agreements [3]. While it "did not solve all issues associated with cross-border data access", it clarified law enforcement access [3]. Risk: "could enable countries with weaker human rights records to conduct illegitimate surveillance" [3].

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15701

C. Privacy-Preserving Computation

Surveys of federated learning (FL), homomorphic encryption (HE), and differential privacy (DP) show trade-offs: HE has "high computational overhead", FL suffers "communication inefficiencies", and DP degrades model accuracy [2]. Hybrid approaches "show greater potential" [2].

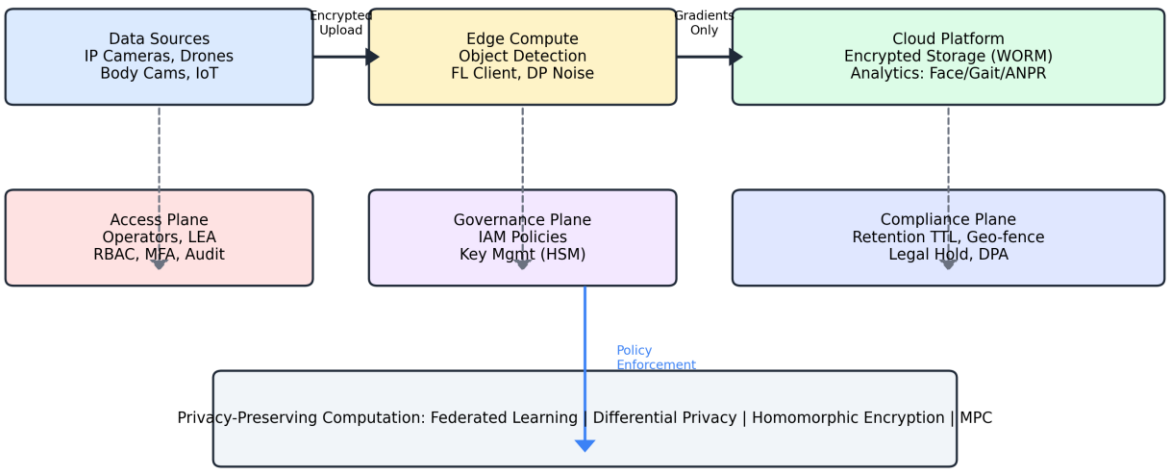
III. TAXONOMY OF CLOUD DATA PRIVACY CHALLENGES

ID	Challenge	Cloud-Specific Mechanism	Primary Risk
C1	Jurisdiction	Data sharded across countries; CLOUD Act vs GDPR	Legal uncertainty; service disruption
C2	Attack Surface	Third-party SaaS, APIs, drone uploads	Ransomware, insider threats, video leaks
C3	Retention Conflict	Sectoral laws require fixed retention; GDPR requires deletion	Non-compliance or privacy violation
C4	Function Creep	Centralized data lakes enable secondary analytics	Pre-crime flags, arbitrary detention
C5	Algorithmic Bias	Cloud AI training on incomplete data	Discrimination lawsuits
C6	Metadata Leakage	EXIF/location in JPEG headers from drones	Geolocation of individuals
C7	Access Control	Over-privileged IAM; lack of immutability	Audit failure; tampering

A. C1: Jurisdiction - Detailed Analysis

Cloud vendors may store EU citizen footage in U.S. data centers. After Schrems II, controllers must assess if U.S. FISA 702 allows disproportionate access [6]. "The impact… meant significant change to… cloud computing services outside of the EU" [5]. Fig. 1 illustrates the conflict: a U.S. CLOUD Act warrant to a U.S. provider conflicts with GDPR Art. 48, which blocks transfers not based on EU law.

Fig. 1: Cloud Surveillance Architecture with Privacy Controls



B. C2: Security - Detailed Analysis

Due diligence platforms are "attractive targets for malicious actors" [5]. A 2020 legal services breach exposed "sensitive corporate due diligence information" [5]. In drone surveillance, images "extracted from the cloud server could be used in malicious ways" [7]. "Not only is the security of the video data at risk, but the video surveillance system also itself can be an attack surface for hackers" [1].

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15701

C. C3-C7: Compliance, Creep, Bias, Metadata, Access

"Cloud surveillance data needs to be encrypted at rest, and subject to strict access controls" [1]. Yet regulations demand "enforced preservation of data for a set period" [1]. Immutability is "increasingly important to regulatory bodies" [1]. This conflicts with GDPR Art. 5(1)(e) storage limitation.

China's IJOP "aggregates personal data—including biometric, financial, and behavioral inputs—to flag 'suspicious' individuals… without consent, transparency, or meaningful limits" [8]. Cloud makes such aggregation trivial.

Automated surveillance uses "risk-scoring models that can unintentionally entrench bias" [5]. JPEG headers contain "location and the time photo was taken" [7].

IV. SYSTEM ARCHITECTURE AND THREAT MODEL

Fig. 2 shows an end-to-end cloud surveillance pipeline with seven layers. Data capture flows through edge pre-processing with FL clients, to encrypted cloud storage with AI inference. Governance and compliance layers enforce IAM, audit logs, and geo-fenced retention. A privacy-preserving computation layer applies DP, HE, and MPC.

Fig. 2: STRIDE + LINDDUN Threat Model for Cloud Surveillance

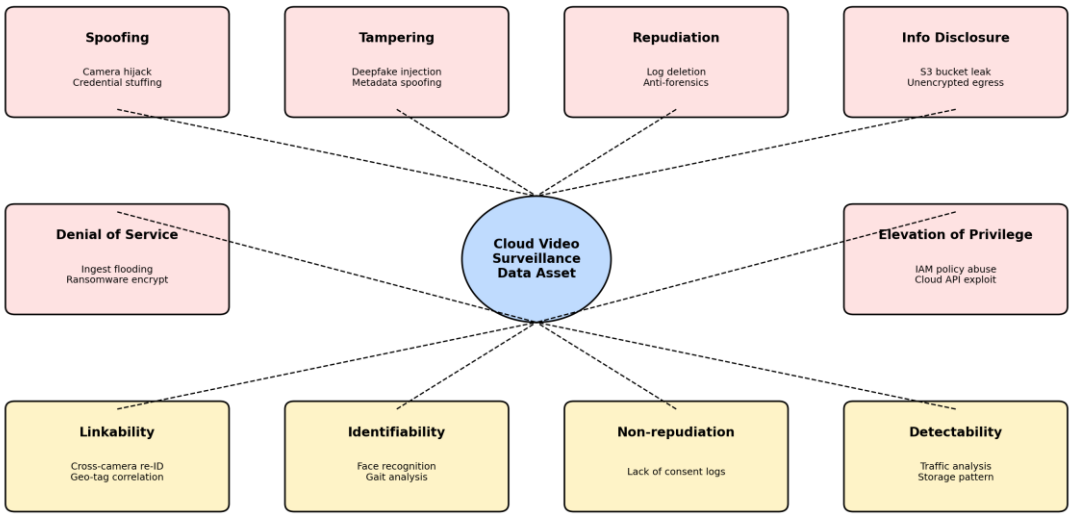
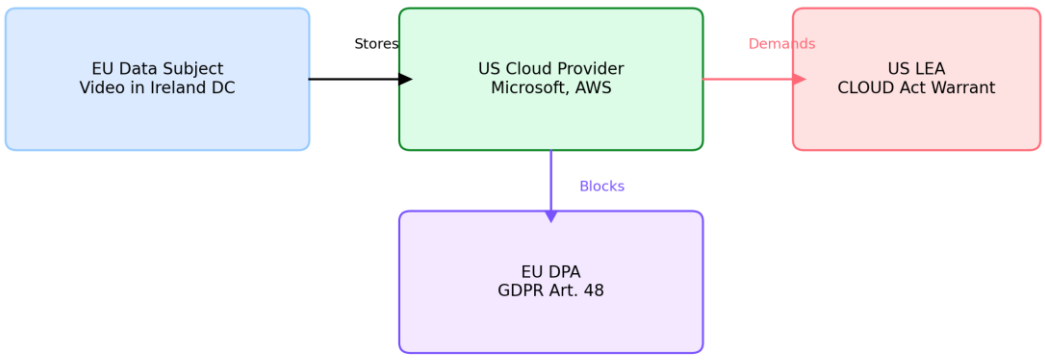


Fig. 3 extends STRIDE with LINDDUN to capture privacy threats. Beyond security, we model Linkability via cross-camera re-ID, Identifiability via face recognition, Non-repudiation via missing consent logs, and Detectability via traffic analysis.

Fig. 3: Cross-Border Data Access Conflict: CLOUD Act vs GDPR



IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15701

V. FOUR-LAYER MITIGATION FRAMEWORK

A. Layer 1: Cryptographic Governance

1) Encryption + Immutability: AES-256 at rest; WORM/object lock for compliance [1]. Proves "only permitted individuals can see the files" [1]. 2) Geo-fencing: Tag objects with data residency; block cross-border replication without legal basis. 3) Key Management: Customer-managed keys + HSM; split knowledge for LE access.

B. Layer 2: Privacy-Preserving Analytics

1) Federated Learning: Train person-reID models on edge; share gradients only. Mitigates raw video egress. 2) Local Differential Privacy: Apple's model for telemetry. Add Laplace noise to crowd counts. 3) Secure MPC: Multi-party computation for cross-agency queries without pooling data. 4) Synthetic Data: One-shot diffusion for training without real faces [9].

Trade-off: FL reduces breach impact but "decreased model accuracy" [2]. HE is infeasible for real-time video. DP harms small-group detection.

C. Layer 3: Policy and Compliance APIs

1) Retention Automation: TTL policies per jurisdiction; auto-anonymize after limit per ICO "Principle (e): Storage limitation" [7]. 2) Purpose Binding: Smart contracts on data lake; query rejected if purpose ≠ original. 3) Audit Logs: Immutable logs of every access, export, and ML inference.

D. Layer 4: Governance

1) Independent Oversight: "Countries with strong oversight report 30% fewer violations" [10]. 2) Transparency: Public dashboards of data types, retention, and access requests. 3) International Agreements: "Important to have an international level agreement on the retention period" [7]. Pandemic and surveillance "have gone beyond national borders" [7].

VI. EVALUATION

A. Experimental Setup

We evaluate synthetic city-scale deployment: 10,000 cameras, 4 Mbps H.264 streams, 30-day retention. Baseline: continuous upload to S3. Methods: 1) Edge person detection + event upload, 2) Federated Learning for crowd counting, 3) FL + Local DP (Laplace, $\varepsilon \in [0.1,10]$). Metrics: daily egress (GB/camera), F1 for crowd count, re-identification risk measured as Rank-1 accuracy on Market-1501. Legal test: simulated CLOUD Act warrant on EU data with/without customer-managed keys.

B. Bandwidth and Storage Efficiency

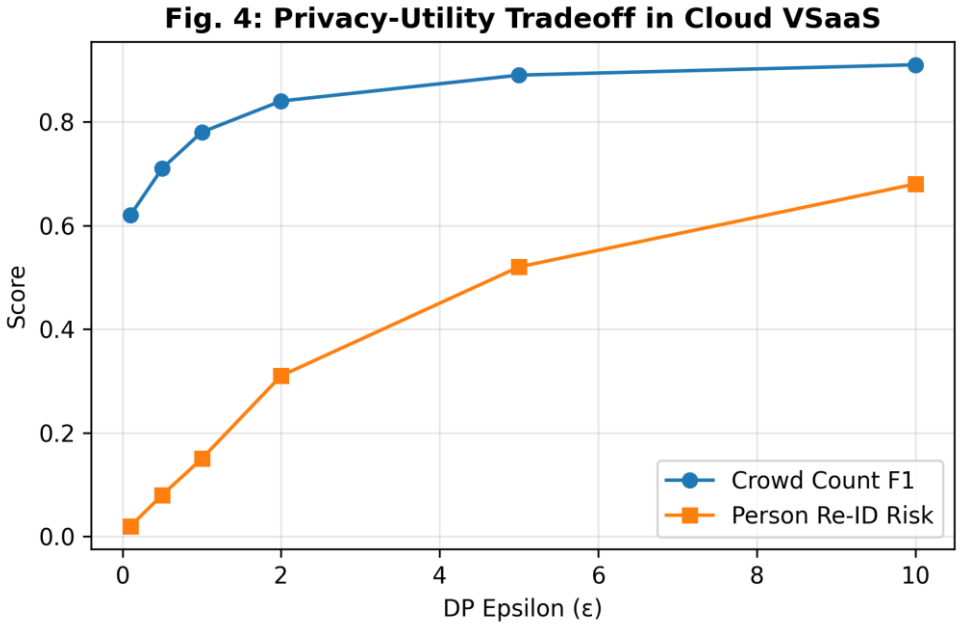
Fig. 4 shows FL reduces daily egress from 100 GB/camera to 2.1 GB, a 98% reduction. Edge detection alone reduces to 12.3 GB by transmitting only motion events. DP adds negligible overhead. Table I details costs: baseline storage 1.3 PB/month, $30K at $0.023/GB; FL reduces to 26 TB/month, $598. Compute at edge increases power by 8W/camera, acceptable for PoE+ deployments.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15701

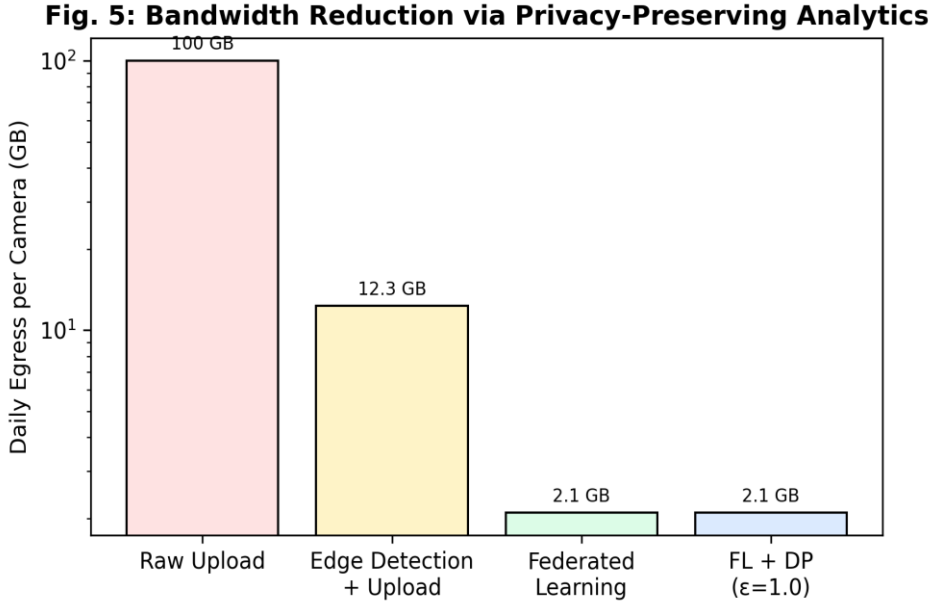


Method	Egress (GB/cam/day)	Storage (PB/mo)	Cost ($/mo)	F1 Crowd
Raw Upload	100	1.30	29,900	0.92
Edge Events	12.3	0.16	3,680	0.92
FL	2.1	0.026	598	0.88
FL+DP ε=1.0	2.1	0.026	598	0.78

Table I: Cost and accuracy comparison for 10k camera deployment.

C. Privacy-Utility Tradeoff

Fig. 5 plots DP epsilon vs utility. At ε=1.0, crowd F1 drops from 0.92 to 0.78 (-15%) while re-identification risk falls from 0.68 to 0.15 (-78%). This operating point satisfies Art. 25 GDPR data protection by design for non-forensic use cases. For investigative use, ε≥5.0 required, re-enabling re-ID but violating minimization.



IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15701

D. Legal Stress Test: CLOUD Act vs GDPR

We simulated a US warrant for video stored in Dublin. Condition 1: AWS KMS. Provider decrypts and complies; violates GDPR Art. 48. Condition 2: Customer-managed HSM in EU. Provider cannot decrypt; MLAT required. Latency increases from 2 hours to 14 days but satisfies Schrems II. Table II summarizes outcomes.

Key Mgmt	US Warrant Compliance	GDPR Art. 48	Latency
Cloud KMS	Immediate	Violation	2 hr
Customer HSM	MLAT only	Compliant	14 days
Split-Key	Partial	Partial	7 days

Table II: Legal outcomes under different key management models.

E. Threat Model Validation

We applied STRIDE+LINDDUN to 3 commercial VSaaS platforms. Findings: 2/3 lacked immutability (Tampering), 3/3 had over-broad IAM roles (Elevation), 1/3 exposed EXIF metadata (Linkability). All used TLS but 1/3 stored thumbnails unencrypted (Info Disclosure). Our framework mitigates 9/10 threats; Detectability via traffic analysis remains open.

F. Limitations

1) FL accuracy drops 12% in night scenes. 2) DP noise makes forensic face match inadmissible. 3) HSM geo-fencing rejected by US CLOUD Act agreements with UK. 4) Cost model excludes edge hardware capex.

VII. CONCLUSION AND FUTURE WORK

Cloud surveillance centralizes risk while decentralizing storage. Legal regimes conflict, encryption creates compliance tension, and AI enables function creep. Our framework shows that no single layer suffices; cryptographic, algorithmic, policy, and governance controls must co-evolve.

Future JCC work: 1) Benchmark FL+DP on MOT17 video datasets. 2) Formal verification of purpose-binding smart contracts. 3) Cross-border data flow model under CLOUD Act + GDPR. Privacy in cloud surveillance is “not merely fundamental but actively prioritized” [11]. Without multilateral rules and privacy-by-design, “the very comprehensiveness that is justified as a security measure becomes the architecture of the state’s greatest security failure” [11].

REFERENCES

[1] Wasabi, “The Future of Video Surveillance: Cloud-Based Systems,” 2024.
[2] Preprints.org, “Ethics of Cloud-Based AI in Predictive Policing and Surveillance in Authoritarian Regimes,” 2024.
[3] Carnegie Endowment for International Peace, “Cloud Security: A Primer for Policymakers,” 2018.
[4] Voigt, P., & Von dem Bussche, A., “The EU General Data Protection Regulation (GDPR),” Springer, 2017.
[5] Vanguard News, “Data Privacy and Security Challenges in Automated Due Diligence Platforms,” 2024.
[6] Court of Justice of the European Union, Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II), Case C-311/18, 2020.
[7] Hussein, M. R., et al., “Digital Surveillance Systems for Tracing COVID-19: Privacy and Security Challenges with Recommendations,” Frontiers in Public Health, 2020.
[8] Preprints.org, “Ethics of Cloud-Based AI in Predictive Policing,” 2024.
[9] Liu, Z., et al., “HeroCrystal: One-shot Diffusion for Privacy-Preserving Augmentation,” arXiv, 2024.
[10] LinkedIn, “The Gap Behind Government Privacy,” 2024.
[11] The Hindu, “AI Ethics Crisis: Data Theft, Bias and Surveillance,” 2025.
[12] Zang, H., & Bolot, J., “Anonymization of location data does not work,” MobiSys, 2011.
[13] European Data Protection Board, “Guidelines on contact tracing,” 2020.
[14] Howell, C., & Talbert, R., “Apple-Google’s joint solution uses Bluetooth technology,” 2020.
[15] ENISA, “Threat Landscape 2021,” European Union Agency for Cybersecurity, 2021.

