Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

UGC CARE II

Integrated Multi-Layer Security Architectures for Cloud-Based Healthcare and Hospitality Systems: A Comprehensive Review and Future Research Agenda

Jitender Singh Harchand
Research Scholar, Malwanchal University, Indore
Dr. Mudita Dave
Research Supervisor, Malwanchal University, Indore

Abstract

Background: The convergence of cloud computing, big data analytics, and digital transformation across healthcare and hospitality has created data environments of extraordinary sensitivity and scale, governed simultaneously by multiple regulatory frameworks and exposed to an increasingly sophisticated threat landscape. Despite extensive research on individual security mechanisms authentication, encryption, access control, intrusion detection, and privacy preservation the academic literature has not produced a unifying architectural framework that integrates these mechanisms into a coordinated multi-layer security system applicable to both healthcare and hospitality cloud environments.

Purpose: This conceptual review critically evaluates the evolution of cloud security architectures, the current state and limitations of core security components, the adequacy of leading cloud security frameworks, and the research challenges that prevent existing approaches from fully addressing the security needs of healthcare and hospitality cloud deployments.

Scope: The review covers authentication mechanisms from passwords through risk-adaptive MFA; access control models from DAC through purpose-based access control; encryption methods from AES-256-GCM through post-quantum CRYSTALS-Kyber; threat detection from signature-based IDS through explainable AI; audit mechanisms from syslog through blockchain-anchored Merkle audit trails; and leading security frameworks including Zero Trust Architecture, NIST CSF, CSA CCM, SASE, Confidential Computing, and XDR. Eight tables provide systematic comparative analysis across 15 architectural approaches and security technique dimensions.

Major Findings: The analysis identifies four critical architectural deficiencies in the current literature: the absence of cross-sector security frameworks addressing both healthcare and hospitality simultaneously; the mechanistic isolation of security components without coordinating intelligence-sharing mechanisms; the systematic underrepresentation of domain-specific insider threat patterns and hospitality-specific attack categories in ML intrusion detection research; and a pervasive reliance on simulation-based evaluation that prevents empirical validation of proposed solutions at production scale. Nine research challenges are characterized including cross-domain interoperability, big data security scalability, dynamic authorization under peak load, adversarial ML, and explainability for regulatory accountability.

Future Directions: The review develops a conceptual roadmap for next-generation integrated multi-layer cloud security architectures and identifies nine priority research directions, including cross-sector architecture design, risk-adaptive authentication, post-quantum cryptography migration, federated intrusion detection, and production-scale deployment validation.

Keywords: *Cloud security architecture; Healthcare informatics; Hospitality technology; Multi-layer security; Zero Trust; Attribute-based encryption; Machine learning intrusion detection; Post-quantum cryptography*

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

1. Introduction

The digital transformation of healthcare and hospitality represents one of the most consequential infrastructure migrations in the history of either industry. Healthcare organizations globally are deploying electronic health record systems, telemedicine platforms, Internet of Medical Things (IoMT) networks, AI-powered diagnostic tools, and national health information exchange infrastructure on cloud platforms that enable unprecedented scale, interoperability, and analytical capability. Simultaneously, hospitality organizations have migrated core operational systems property management, revenue analytics, customer relationship management, and loyalty programme platforms to cloud-native architectures that support real-time multi-property management and sophisticated guest analytics. Both migrations have been accelerated by regulatory mandates, competitive pressure, and the operational lessons of the COVID-19 pandemic, which simultaneously demonstrated both the life-critical importance of digital health infrastructure and the catastrophic operational consequences of cybersecurity failures in cloud environments (Kwon & Johnson, 2021; Verizon, 2023).

The security challenge created by this convergence is substantial and increasing. Healthcare experiences the highest mean data breach cost of any industry sector USD 10.93 million per incident in 2023 (IBM Security, 2023) reflecting the combination of regulatory penalties, extended remediation timelines, and reputational damage that healthcare breaches incur. Hospitality has experienced multiple large-scale incidents, most notably the Marriott International breach that exposed 500 million guest records (Information Commissioner's Office, 2020) and exposed the systemic vulnerability of legacy PMS infrastructure to cloud-era attack techniques. The Verizon (2023) Data Breach Investigations Report identifies credential theft, API exploitation, and ransomware as the three dominant breach categories in both sectors, reflecting a threat landscape that has evolved substantially beyond the perimeter-focused security architectures that most organizations deployed a decade ago.The academic response to this security challenge has been substantial in volume but fragmented in scope. A large body of research addresses individual security mechanisms Li et al. (2013) on CP-ABE for healthcare sharing; Singh et al. (2022) on deep learning ensemble IDS; Dwork and Roth (2014) on differential privacy; Wazid et al. (2020) on lightweight authentication for IoMT without integrating these mechanisms into coordinated architectures that address the complete spectrum of threats facing cloud-hosted healthcare and hospitality systems. Equally important, existing research predominantly addresses either healthcare or hospitality, not both, despite the structural similarity of their security challenges and the growing number of organizations medical tourism facilities, wellness hospitality providers, telemedicine-adjacent accommodation services that must protect both data categories simultaneously.

This conceptual review addresses this gap by providing a comprehensive critical analysis of cloud security architectures and their adequacy for healthcare and hospitality cloud deployments. The review's analytical objectives are: to trace the historical evolution of cloud security architecture and identify the trends shaping next-generation approaches; to critically evaluate the current state of each core security component and the specific limitations that prevent individual mechanisms from providing adequate integrated protection; to compare leading cloud security frameworks against the specific requirements of healthcare and hospitality deployments; to characterize the research challenges that define the frontier of the field; and to develop a conceptual roadmap for next-generation

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

integrated multi-layer security architectures that addresses the identified limitations.

The review is organized as follows. Section 2 traces the evolution of cloud security architectures from perimeter-based approaches through Zero Trust to emerging cloud-native paradigms. Section 3 critically reviews each core security component authentication, access control, encryption, secure sharing, threat detection, and audit with explicit evaluation of healthcare and hospitality applicability. Section 4 compares leading cloud security frameworks. Section 5 presents the comparative architecture evaluation. Section 6 characterizes nine research challenges. Section 7 develops the conceptual future research roadmap. Section 8 discusses emerging technologies. Section 9 concludes.

2. Evolution of Cloud Security Architectures

2.1 From Perimeter Security to Zero Trust

The evolution of cloud security architecture over the past three decades can be characterized as a progressive deconstruction of the implicit trust assumptions that underlay traditional perimeter-based security. Traditional enterprise security, dominant through the 1990s and early 2000s, operated on the castle-and-moat principle: external network perimeters were fortified with firewalls, intrusion detection systems, and network access controls, while traffic within the perimeter was treated as implicitly trustworthy. This architecture was adequate when corporate data resided on on-premise servers and users accessed data through dedicated internal networks, but it failed catastrophically when cloud adoption, mobile computing, and bring-your-own-device policies eliminated the geographic and network boundaries that defined the protected perimeter.

The Defence in Depth principle (Saltzer & Schroeder, 1975) represented the first significant architectural response to perimeter security's limitations, recognizing that reliance on a single security barrier creates a single point of failure and that effective security requires multiple independent layers, each addressing a distinct threat category. Defence in Depth established the conceptual foundation for modern multi-layer security architectures the recognition that authentication, authorization, encryption, monitoring, and logging must operate as independent, complementary layers rather than as optional additions to a primary perimeter control. The principle's theoretical validity has been consistently confirmed in practice: data breach investigations routinely find that successful attacks exploit the absence or failure of specific security layers that would have been sufficient to prevent compromise if present (Verizon, 2023).

Zero Trust Architecture (ZTA), articulated by Kindervag (2010) and formalized by NIST (Rose et al., 2020), represents the most significant paradigm shift in cloud security architecture of the past decade. ZTA's core principle that no entity, user, device, or network location should be implicitly trusted and that every access request should be explicitly verified against current policy regardless of its origin directly addresses the fundamental inadequacy of perimeter-based security in cloud environments where the very concept of a trustworthy internal network no longer applies. NIST SP 800-207's seven tenets of Zero Trust provide an authoritative architectural specification: all data sources and computing services are considered resources; all communication is secured regardless of network location; access to individual resources is granted per-session; access policy is dynamic and based on client identity and behavioural attributes; integrity and security posture of all owned assets is monitored; authentication and authorization are strictly enforced; and information about assets and network infrastructure is used to improve security posture.

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

The practical implementation of ZTA in healthcare and hospitality environments has proven more complex than the principle suggests. Healthcare deployments face legacy integration challenges: older clinical information systems laboratory information systems, radiology information systems, pharmacy management systems were designed for implicit-trust internal network environments and lack the API-level authentication and authorization capabilities required by strict ZTA implementations. Hospitality deployments face supply chain complexity: the typical hotel technology stack integrates 15–20 third-party systems (PMS, CRS, revenue management, point-of-sale, housekeeping management, door lock systems) from different vendors, each with independent authentication and authorization models that are difficult to integrate under a unified ZTA policy. These practical constraints suggest that ZTA is a necessary but not sufficient architectural principle, and that effective cloud security for healthcare and hospitality requires domain-specific implementations that extend ZTA's principles with context-specific authentication calibration, domain-aware access control policies, and sector-specific threat detection capabilities.

2.2 Cloud-Native Security, SASE, and Confidential Computing

The emergence of cloud-native security architectures represents the current frontier of security evolution, characterized by three advances beyond traditional ZTA implementations: the integration of security functions into the cloud service fabric itself (cloud-native security); the convergence of networking and security into a unified cloud-delivered service (Secure Access Service Edge, SASE); and the extension of cryptographic protection to data in use during computation (Confidential Computing). Cloud-native security, enabled by container orchestration platforms (Kubernetes), service mesh architectures (Istio), and cloud provider security services (AWS Security Hub, Azure Sentinel), enables security controls to be embedded directly in application workload deployment rather than applied through separate security infrastructure, providing more granular and dynamic security policy enforcement than perimeter-based approaches.

SASE, defined by Gartner and implemented by cloud security vendors including Palo Alto Networks Prisma Access, Zscaler, and Cisco Umbrella, converges wide-area networking (SD-WAN) with cloud-delivered security services (secure web gateway, cloud access security broker, zero trust network access, firewall-as-a-service) into a unified cloud architecture. For hospitality organizations managing security across hundreds or thousands of geographically distributed properties, SASE's cloud-delivery model offers significant operational advantages over maintaining independent security infrastructure at each property. For healthcare organizations managing distributed clinical facilities, telemedicine endpoints, and IoMT device networks, SASE's unified policy enforcement across all access points addresses the network complexity that makes consistent ZTA implementation difficult.

Confidential Computing the use of hardware-isolated Trusted Execution Environments (TEEs) such as Intel SGX, AMD SEV, and ARM TrustZone to protect data in use during computation addresses a fundamental gap in the classic encryption model: while data can be encrypted at rest and in transit, it must be decrypted for computation, creating a window of vulnerability during which plaintext data is exposed to the cloud provider's infrastructure. Confidential Computing eliminates this window by performing computation on encrypted data within a hardware-isolated TEE that is protected from the cloud provider's hypervisor and operating system. For healthcare cloud analytics processing encrypted patient records within a TEE such that the cloud provider cannot observe the plaintext

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025
IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business
UGC CARE II

Confidential Computing provides a compelling security model that addresses both insider threat (cloud provider employee access) and legal jurisdiction concerns. The primary barrier to widespread healthcare and hospitality adoption is performance overhead: TEE-based computation currently imposes 10–50% performance costs that may be unacceptable for latency-sensitive clinical applications.

2.3 Security-by-Design and Privacy-by-Design

The security-by-design principle the integration of security considerations into system architecture from the earliest design stages rather than through post-hoc addition of security controls has gained regulatory force through GDPR Article 25's data protection by design and by default requirement and HIPAA's implementation specifications. Security-by-design for cloud healthcare and hospitality architectures implies three specific design requirements: that sensitive data is encrypted before cloud storage as the default state rather than an optional configuration; that access control policies enforce minimum necessary access as the default rather than requiring explicit restriction; and that security event logging is comprehensive and immutable from system initialization rather than being enabled only after a security incident. These requirements have fundamental implications for the architecture of cloud security systems, prioritizing cryptographic enforcement of security properties over procedural or administrative controls that can be bypassed or misconfigured.

3. Core Security Components: Critical Analysis

3.1 Authentication

Authentication the process of verifying that an entity claiming an identity is in fact that entity is the foundational security function on which all subsequent access control and authorization decisions depend. The adequacy of an authentication mechanism is evaluated across four criteria: security strength (resistance to known attack techniques), usability (the operational friction imposed on legitimate users), scalability (the computational and administrative cost of deploying the mechanism at organizational scale), and regulatory alignment (compliance with the authentication requirements of applicable regulations). Table 1 provides a systematic comparison of authentication techniques along these dimensions.

Table 1: Authentication Technique Comparison Security, Usability, and Domain Applicability

Method	Mechanism	NIST AAL	Healthcare Fit	Hospitality Fit	Key Strength	Critical Weakness
Password (Knowledge)	Shared secret hash comparison	AAL1	Low (99.9% of breaches exploit passwords)	Low	Universal familiarity; zero hardware cost	Phishing; stuffing; reuse; no context

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

TOTP / HOTP	HMAC(seed ‖ time/counter) mod 10^6	AAL2	Moderate (SIM swap risk)	Moderate	Widely supported; low cost	SIM swap; real-time phishing; seed theft
FIDO2 / WebAuthn	ECDSA challenge-response + hardware	AAL3	High (phishing-resistant)	High	Phishing-immune; no server-side secret	Hardware cost; UX complexity; PKI mgmt
Biometric (fingerprint/face)	Template matching; liveness detection	AAL2–3	High (clinical efficiency)	High (guest experience)	Fast; frictionless for high-sensitivity	Irrevocability; spoofing; GDPR biometric data
Risk-Adaptive MFA (RAAA)	Context scoring × factor calibration	AAL1–3	Very High (workflow-compatible)	Very High	Dynamic security/usability balance	Model cold-start; adversarial adaptation
Passwordless (passkey)	Platform authenticator + FIDO2	AAL2	Emerging (ABDM alignment)	Emerging (guest apps)	No phishing surface; synced credentials	Account recovery complexity; ecosystem lock-in
SSO / Federated (OIDC)	OAuth 2.0 + OpenID Connect	AAL2	High (EHR integration)	High (PMS/OTA federation)	Single credential; reduced helpdesk	IdP single point of failure; token theft

Note. NIST AAL = Authentication Assurance Level per NIST SP 800-63B. HC = Healthcare; HT = Hospitality. Risk-Adaptive MFA refers to contextually calibrated multi-factor authentication that adjusts factor requirements based on real-time risk scoring. 'Production' deployment maturity indicates widespread deployment in commercial or clinical environments.

The critical analytical finding from Table 1 is that no single authentication mechanism optimizes across all four criteria simultaneously. Password-only authentication fails the security criterion (compromised in 99.9% of automated credential attacks, per Lee, 2019) but satisfies the usability and scalability criteria that make it pervasive despite its inadequacy. FIDO2/WebAuthn hardware security keys satisfy the security criterion at NIST AAL3 level and are phishing-resistant in a way that TOTP-based authentication is not a FIDO2 authentication ceremony cannot be intercepted by a real-time phishing proxy because the challenge response is domain-bound but impose hardware cost and administrative complexity that limits deployment in large, staff-diverse healthcare and hospitality organizations. Biometric authentication provides the frictionless high-assurance experience

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

that clinical and hospitality workflows demand but raises irrevocability and biometric data protection concerns that are particularly significant under GDPR's explicit prohibition on biometric data processing without explicit consent.

Risk-adaptive authentication in which authentication factor requirements are calibrated in real-time to the contextual risk of the specific access request emerges from the analysis as the theoretically optimal approach for healthcare and hospitality contexts, because it achieves the security strength of high-assurance multi-factor authentication for high-risk access events while maintaining the low friction of single-factor authentication for low-risk routine access. The implementation challenge is the design of the risk scoring model: the contextual signals used to assess access risk (location, device security posture, temporal anomaly, behavioural deviation) require individual historical baseline models that take time to develop and may be manipulated by sophisticated adversaries who gradually shift the risk scoring baseline through a period of normal-pattern access. Bonneau et al. (2012) provide the foundational theoretical framework for authentication scheme comparison; NIST SP 800-63B (NIST, 2017) provides the authoritative standard for authentication assurance levels that should govern healthcare and hospitality authentication requirements.

3.2 Access Control

Access control the enforcement of policies that restrict which entities may perform which operations on which resources under which conditions is the architectural component most directly responsible for implementing the least privilege principle that lies at the heart of healthcare and hospitality data protection requirements. The evolution from Discretionary Access Control (DAC) through Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and toward Risk-Adaptive and Purpose-Based Access Control reflects a progressive increase in policy expressiveness accompanied by increasing implementation complexity. Table 2 presents the comparative analysis.

Table 2: Access Control Model Comparison Granularity, Expressiveness, and Domain Suitability

Model	Decision Basis	Granularity	HC Application	HT Application	Strengths	Critical Limitations
DAC (Discretionary)	Owner-granted permissions	Object-level	Research data sharing (limited)	File-share scenarios	Flexible; user-controlled	No accountability; delegation risks
MAC (Mandatory)	System-enforced labels	Clearance level	Military/govt health data	Classified hotel security	Strong coercive enforcement	Inflexible; no context; administrative overhead
RBAC	Organizational role	Role + object type	Clinician roles (Physician/Nurse)	Staff roles (Manager/Receptionist)	Simple administration; scalable	Role explosion; no context; BOLA-vulnerable

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

ABAC	Subject + resource + env attributes	Data element	Purpose-limited PHI access	Property-limited guest data	Fine-grained; context-sensitive; GDPR-ready	Policy complexity; evaluation latency
Hybrid RBAC/ABAC	Role pre-filter + attribute evaluation	Element + context	Clinical workflow-optimized HC	Cross-property HT access	Balances simplicity and granularity	Dual administration; integration complexity
Risk-Adaptive AC	Role + attributes + live risk score	Element + purpose	Emergency escalation; insider threat	Anomalous transaction gating	Dynamic security posture; workflow-aware	Risk model accuracy; adversarial score gaming
PBAC (Purpose-Based)	Declared data use purpose	Purpose scope	HIPAA minimum necessary	GDPR purpose limitation	Regulatory natural fit	Purpose verification challenge; consent management

Note. 'Granularity' refers to the finest data unit at which the access control model can meaningfully restrict access. HC = Healthcare; HT = Hospitality. Risk-Adaptive AC represents the most advanced current model, combining RBAC/ABAC with real-time risk score integration in the access decision function.

RBAC's dominance in current healthcare and hospitality deployments reflects its administrative simplicity and its alignment with organizational structures mapping clinical roles (Physician, Nurse, Pharmacist, Radiologist) or hospitality roles (Front Desk, Housekeeping, Revenue Manager) to permission sets is an intuitive administrative task that fits within existing HR management workflows. However, RBAC's limitations become critical at the data element level: a Physician role that grants access to all patient data within the role's scope cannot implement the minimum necessary principle required by HIPAA for situations in which the physician requires only a specific element (the medication list or the allergy record) from a patient record containing many sensitive elements. The role explosion problem in which RBAC attempts to approximate fine-grained access control through proliferating specialized roles creates administrative overhead that grows quadratically with the number of role-permission combinations required.

ABAC's context-sensitive policy evaluation addresses RBAC's granularity limitation but introduces evaluation latency as the primary operational concern. A complex ABAC policy evaluated against a large attribute set using a software policy evaluation engine may require 50–200 ms per decision potentially unacceptable in clinical workflows requiring rapid sequential data access. The

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

open-source Open Policy Agent (OPA) with Rego policy language, compiled to WebAssembly for hardware-accelerated evaluation, represents the current state of the art in ABAC implementation, achieving sub-50 ms evaluation latency for typical healthcare and hospitality policies. The hybrid RBAC/ABAC approach using RBAC for a fast pre-filtering step that eliminates obviously unauthorized requests before ABAC evaluation reduces the number of requests reaching the computationally expensive ABAC evaluation, achieving better latency performance than pure ABAC while retaining ABAC's fine-grained control capability.

3.3 Encryption

Encryption provides cryptographic enforcement of data confidentiality, ensuring that data is computationally infeasible to read without the appropriate decryption key regardless of how the data was obtained whether through authorized API access, misconfiguration-exposed storage access, or physical hardware seizure. The diversity of encryption algorithms, modes, and key sizes available to cloud security architects requires systematic evaluation against the specific requirements of healthcare and hospitality use cases. Table 3 provides this evaluation.

Table 3: Encryption Method Comparison Performance, Suitability, and Post-Quantum Readiness

Algorithm	Type	Key Size / Mode	Throughput	HC Suitability	HT Suitability	Post-Quantum Safe	Primary Limitation
AES-256-GCM	Symmetric AEAD	256-bit; GCM	600+ MB/s (AES-NI)	Very High (PHI at rest)	Very High (PAN storage)	Yes (key exchange needs PQC)	Key management at scale
ChaCha20-Poly1305	Symmetric AEAD	256-bit; AEAD	400+ MB/s (no hw accel)	High (IoMT / mobile)	High (smart room IoT)	Yes	Less hardware support than AES
RSA-2048/4096	Asymmetric	2048/4096-bit	~1 KB/s (sign/verify)	Moderate (legacy PKI)	Moderate (TLS certs)	No (Shor's algorithm)	Quantum-vulnerable; slow; large keys
ECDH / ECDSA (P-256)	Asymmetric / Signature	256-bit (ECC)	14K+ ops/sec	High (TLS; JWT signing)	High (API auth)	No (ECDLP → quantum)	Quantum-vulnerable; proprietary curve concerns
CP-ABE (BSW09)	Attribute-based	Pairing-based; variable	200–800 ms / op	High (EHR sharing)	High (OTA data sharing)	Partially (needs PQC-ABE)	High computational cost; key revocation

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

BFV / CKKS (FHE)	Homomorphic	Variable; large ciphertext	10^3–10^6× overhead	Emerging (clinical analytics)	Emerging (guest analytics)	Yes (lattice-based)	Extreme performance cost; bootstrapping complexity
CRYSTALS-Kyber (FIPS 203)	PQC KEM	ML-KEM-768 (3 security)	~1 ms key gen/encap	Critical (future PHI)	Critical (future PAN)	Yes (NIST standardised 2024)	Larger key/ciphertext sizes; ecosystem immaturity
CRYSTALS-Dilithium (FIPS 204)	PQC Signature	ML-DSA-65 (3 security)	~0.5 ms sign/verify	Critical (future audit sigs)	Critical (future auth)	Yes (NIST standardised 2024)	Larger signature sizes vs ECDSA

Note. Throughput values are approximate and hardware-dependent; AES-256-GCM values assume AES-NI hardware acceleration (Intel Xeon Platinum). CP-ABE latency depends on policy complexity (number of attributes). FHE overhead range reflects variation across scheme types and operation complexity. PQC = Post-Quantum Cryptography; NIST 2024 indicates standardization in 2024 FIPS publications.

The encryption landscape for healthcare and hospitality cloud security is currently in a transitional state driven by the NIST post-quantum cryptography standardization process, which finalized CRYSTALS-Kyber (FIPS 203) for key encapsulation and CRYSTALS-Dilithium (FIPS 204) for digital signatures in 2024. The immediate implication is that current asymmetric cryptography RSA and ECDH/ECDSA is known to be vulnerable to attacks by cryptographically relevant quantum computers using Shor's algorithm. While commercially available quantum computers cannot yet execute Shor's algorithm on the key sizes used in practice, the 'harvest now, decrypt later' attack strategy in which adversaries collect encrypted healthcare and financial data today for future decryption when quantum hardware matures creates an immediate threat to long-lived sensitive data. Healthcare patient records must be protected for the patient's lifetime (potentially 80+ years); hospitality payment and identity data has long-term fraud implications. This temporal asymmetry between the expected quantum computing timeline (10–15 years for cryptographically relevant systems) and the data retention periods in these sectors creates a case for beginning PQC migration immediately, even before quantum computers can actually break current cryptography.

CP-ABE's role in inter-organizational data sharing deserves critical examination in this transitional context. The BSW09 CP-ABE scheme (Bethencourt et al., 2007) is based on bilinear pairing operations over elliptic curves, which like ECDH and ECDSA are vulnerable to quantum computing attacks. Developing post-quantum CP-ABE alternatives that preserve the policy-embedding property of existing CP-ABE while providing quantum resistance is an active research area, with

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

lattice-based ABE constructions representing the most promising direction. The practical implication for healthcare and hospitality organizations deploying CP-ABE-based sharing protocols today is that they should architect these systems with algorithm agility the ability to replace the underlying ABE scheme without architectural redesign to facilitate migration when quantum-safe ABE schemes mature.

3.4 Secure Data Sharing

Data sharing across organizational boundaries between hospitals and referring providers, between hotels and OTA partners, between tourism operators and destination management organizations is a fundamental operational requirement in both sectors, but it simultaneously represents one of the most significant attack surfaces for data exposure. Effective secure data sharing mechanisms must provide three properties: identity verification that the recipient is who they claim to be; access policy enforcement that the recipient can access only the specific data elements authorized for the specific sharing purpose; and data minimization that only the minimum necessary data is transmitted to the recipient. Conventional TLS-based API sharing satisfies the identity verification requirement through certificate-based authentication but fails the access policy enforcement and data minimization requirements, because TLS protects data in transit but does not restrict what data is transmitted once the transport connection is authenticated.

CP-ABE addresses this limitation by embedding the access policy directly in the ciphertext encryption, such that a recipient can only decrypt the data if their attribute credentials satisfy the policy making unauthorized access computationally infeasible rather than procedurally controlled. Proxy Re-Encryption (PRE) extends this by enabling a trusted proxy to transform ciphertext encrypted for one key into ciphertext decryptable by a different key, enabling dynamic re-delegation of decryption authority without exposing the underlying plaintext. The combination of CP-ABE for policy enforcement and PRE for delegation provides a cryptographically complete sharing model that has been demonstrated in healthcare contexts (Li et al., 2013; Abdulsalam & Hedabou, 2022) but has not been extended to hospitality or tourism data sharing scenarios a specific gap identified in this review's research agenda.

3.5 Intelligent Threat Detection

The evolution from signature-based IDS to ML-ensemble, deep learning, and UEBA-based threat detection represents perhaps the most consequential technical advance in cloud security of the past decade, enabling the detection of sophisticated attacks particularly insider threats and advanced persistent threats that are structurally invisible to signature-based approaches. Table 5 provides the comparative technical analysis of detection approaches.

Table 5: Threat Detection Technique Comparison Detection Capability and Domain Suitability

Technique	Detection Approach	HC Effectiveness	HT Effectiveness	Novel Attack ADR	False Positive Rate	Deployment Maturity
Signature-based IDS	Pattern matching vs	Low (insider	Low (novel booking	Near-zero	Very Low (< 1%)	Production (legacy)

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

	known signatures	misuse invisible)	fraud missed)			
Anomaly-based IDS (statistical)	Deviation from statistical baseline	Moderate (drift detection)	Moderate	Moderate (~60%)	Moderate (3–8%)	Production
ML Ensemble (RF + XGBoost)	Feature learning from labelled attack data	High (known attack patterns)	High (fraud pattern detection)	High (> 90% known variants)	Moderate (2–5%)	Production -ready
LSTM Sequential Detection	Temporal sequence pattern learning	Very High (insider EHR misuse)	High (slow loyalty fraud)	High (APT; insider sequences)	Moderate (3–6%)	Research → Production
Autoencoder Anomaly Detection	Reconstruction error from normal model	High (novel attack zero-day)	High (novel booking patterns)	High (novel attacks)	Higher (5–10%)	Research → Production
UEBA (User Entity Behaviour)	Individual-baseline deviation scoring	Very High (insider; privilege abuse)	Very High (account takeover)	Very High (insider)	Low (personalised baseline)	Production (enterprise)
Federated IDS	Cross-org FL without data sharing	High (cross-hospital threats)	High (chain-wide fraud)	High (collective intelligence)	Low–Moderate	Research phase
Explainable AI IDS (SHAP/LIME)	Attribution + ML detection combined	High + interpretable	High + interpretable	High	Moderate	Research → Emerging

Note. ADR = Attack Detection Rate (recall/true positive rate). Values are representative ranges based on benchmark evaluations; actual performance in specific HC/HT deployments will vary with data characteristics and attack profile. UEBA baselines require minimum 30–90 days of historical data; cold-start detection rates are lower than shown.

The LSTM sequential model's superior performance on insider threat and APT detection scenarios categories that dominate healthcare and hospitality breach statistics reflects the fundamental insight that these attack categories manifest as sequences of individually innocuous events rather than as individual anomalous events. An insider browsing unauthorized patient records may access each record with valid credentials and authorized API calls; it is only the temporal sequence and cumulative volume of accesses outside the user's normal clinical scope that reveals the misuse. LSTM's ability to model arbitrary-length temporal sequences and detect deviations from the normal sequence distribution

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

makes it uniquely suited to this detection challenge, but it requires sufficient historical data to train a meaningful normal sequence model a cold-start problem that is particularly acute for healthcare organizations deploying ML IDS in environments without existing labelled security event datasets.

The false positive rate is the operationally limiting factor for ML IDS deployment in clinical and hospitality environments, not the detection rate. Garg et al. (2020) achieve detection rates exceeding 0.97 with false positive rates of 3–5% which would generate approximately 3,000–5,000 false alarms per 100,000 normal events. In a large hospital or hotel chain processing millions of daily events, this translates to tens of thousands of daily false alarms a volume that would create the alert fatigue that makes genuine threats invisible. Future ML IDS research for healthcare and hospitality contexts should weight false positive rate reduction at least as heavily as detection rate improvement, and should evaluate performance on domain-specific datasets that reflect the actual distribution of normal versus anomalous events in clinical and hospitality environments.

3.6 Audit and Compliance

Audit logging the creation of comprehensive, tamper-evident records of all security-relevant events serves four distinct functions in healthcare and hospitality cloud environments: regulatory compliance (HIPAA requires audit controls for all PHI access; PCI DSS requires audit log retention for all cardholder data environment access); forensic investigation (audit logs provide the evidence base for reconstructing security incidents); user accountability (non-repudiable audit records create accountability for data access decisions); and continuous monitoring (real-time analysis of audit logs enables detection of anomalous access patterns that may indicate insider misuse or active attacks). The technical requirements for audit logging in cloud environments extend beyond those of traditional syslog: cloud audit logs must be tamper-evident (modification of historical records must be detectable), append-only (no audit record can be deleted), cryptographically attributable (each record must be signed with the generating component's key), and retained for the regulatory retention period (HIPAA requires six years; PCI DSS requires one year immediately accessible).

Blockchain-anchored audit logging in which Merkle root hashes of audit log batches are published to an external blockchain for independent verification provides the maximum tamper-evidence property: even if the audit log storage is compromised, any modification will produce a Merkle hash that doesn't match the externally verified root, enabling detection. However, public blockchain publication introduces latency and gas cost concerns for healthcare and hospitality organizations processing millions of audit events per day. Permissioned blockchain architectures (Hyperledger Fabric) or periodic publication of daily Merkle roots to an immutable external reference represent practical alternatives that achieve the tamper-evidence objective with lower operational overhead.

4. Existing Cloud Security Frameworks: Critical Comparison

The cloud security framework landscape encompasses standards-based specifications, vendor-defined architectural patterns, and academic research proposals, each addressing different aspects of the integrated security challenge. Table 4 provides a systematic comparison of eight leading frameworks against the specific requirements of healthcare and hospitality deployments.

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

Table 4: Cloud Security Framework Comparison Completeness and Domain Suitability

Framework	Governing Body	Core Principle	HC Support	HT Support	Big Data	Strengths	Limitations
Zero Trust Architecture (NIST SP 800-207)	NIST	Never trust, always verify; micro-segment	Moderate	Moderate	Moderate	Eliminates implicit trust; policy-driven	Implementation complexity; legacy incompatibility
NIST Cybersecurity Framework (CSF 2.0)	NIST	Identify-Protect-Detect-Respond-Recover	High (HIPAA mapping)	High (PCI mapping)	Moderate	Flexible; regulatory-aligned; risk-based	Guidance only; no implementation spec
CSA Cloud Controls Matrix v4	Cloud Security Alliance	197 cloud-specific controls across 17 domains	High (HIPAA/GDPR mapping)	High (PCI DSS mapping)	High	Cloud-native; comprehensive mapping	Self-certification limitations; complexity
SASE (Secure Access Service Edge)	Gartner	Network + security = cloud service	Moderate (WAN-centric)	High (multi-property WAN)	High	Converges network and security; cloud-native	Vendor lock-in; cost; emerging maturity
Confidential Computing	CCC (Linux Foundation)	TEE-based data-in-use protection	High (EHR analytics in cloud)	Moderate	Moderate	Hardware-rooted trust; data-in-use security	Hardware dependency; performance overhead; complexity
XDR (Extended Detection & Response)	Multiple vendors	Cross-layer telemetry correlation	High (clinical SOC)	High (hotel SOC)	High	Holistic threat visibility; automation	Vendor proprietary; integration costs
AI-Assisted Security (e.g.	Multiple vendors	LLM + ML for threat detection	Emerging	Emerging	High	Natural language queries; automated	Explainability; adversarial ML;

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

Google SecAI)		and response				response	hallucination risk
Privacy-Enhancing Technologies (PETs)	ISO/IEC; NIST	DP + FL + SMC for privacy-safe analytics	High (clinical analytics)	Emerging (guest analytics)	High	Mathematical privacy guarantees	Utility degradation; calibration expertise required

Note. HC Support and HT Support ratings reflect the framework's explicit coverage of domain-specific requirements (HIPAA, GDPR, PCI DSS) and domain-specific threat scenarios, not just generic cloud security coverage. 'Moderate' indicates partial coverage requiring domain-specific extension; 'High' indicates substantial native coverage.

The comparative analysis reveals a critical architectural gap across all eight frameworks: none provides the integrated, coordinated combination of domain-specific authentication, fine-grained access control, policy-enforced data sharing, ML-based domain-specific threat detection, privacy-preserving analytics, and immutable audit logging that comprehensive healthcare and hospitality cloud security requires. ZTA (NIST SP 800-207) provides the foundational architectural principle but lacks domain-specific implementation guidance and does not address CP-ABE-based secure sharing or differential privacy analytics. The NIST CSF 2.0 provides excellent regulatory mapping but is explicitly a guidance framework rather than an implementation specification. The CSA CCM v4 provides the most comprehensive cloud-specific control specification but remains a control catalogue rather than an architectural design. SASE and XDR provide strong operational capabilities but are vendor-proprietary and lack the domain-specific healthcare and hospitality policy layers required for regulatory compliance.

The absence of a framework that integrates all required security dimensions reflects the same fragmentation that characterizes the academic literature: each framework excels in specific dimensions (ZTA in access policy; CSA CCM in control comprehensiveness; SASE in network security; XDR in threat detection) but no single framework provides the integrated coordination across all dimensions that cloud-hosted healthcare and hospitality data requires. This integration gap the absence of an architectural framework that specifies not just what security controls are needed but how they coordinate through shared intelligence to provide emergent security properties greater than the sum of their individual contributions is the primary architectural research challenge identified by this review.

5. Comparative Evaluation of Security Architectures

Table 6 presents the comparative evaluation of 15 security architectures and frameworks against the key dimensions required for comprehensive healthcare and hospitality cloud security. The comparison includes both academic research proposals and commercial/standards frameworks, evaluated on authentication, access control, encryption, threat detection, audit logging, scalability, and domain applicability dimensions.

Table 6: Integrated Security Architecture Comparison 15 Architectures Across 11 Dimensions

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

Architecture / Study	Auth	Access Ctrl	Encryption	Threat Det.	Audit	Scalability	HC ✓	HT ✓	Big Data ✓	Primary Gap
Traditional Perimeter (pre-2015)	Password	RBAC	TLS only	Signature IDS	Syslog	Low	Partial	Partial	No	No cloud awareness; no insider detection
Zero Trust (NIST SP 800-207)	MFA	RBAC/ABAC	TLS 1.3	Behavioural	Policy log	Moderate	Partial	Partial	Partial	No domain-specific encryption; no privacy layer
CSA CCM v4 Framework	MFA	ABAC	AES-256	SIEM	Immutable	High	Partial	Partial	High	Guidance only; no cross-sector integration
Li et al. (2013) – HC CP-ABE	Basic	CP-ABE policy	CP-ABE	None	None	Low	Yes	No	No	No IDS; no HT; no audit trail
Wazid et al. (2020) – IoMT Auth	Lightweight MFA	RBAC	AES	None	Basic	Low	Yes	No	No	No ABAC; no big data; HC only
Abdulsalam & Hedabou (2022)	Token	ABE	ABE+AES	None	Blockchain	Low	Yes	No	No	No IDS; no HT domain
Garg et al. (2020)	None	None	None	DL ensemble	None	High	No	No	Yes	No auth/access/encryption

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

– DL IDS										layers
Diro & Chilamkurti (2018) – FL IDS	None	None	None	Federated DNN	None	High	No	No	Yes	No domain application; auth/encrypt absent
Kumari et al. (2023) – FL HC	Basic	Role	DP	Partial	None	Moderate	Yes	No	High	No access control; no HT scope
Rathore et al. (2021) – Blockchain IoT	Token+BC	SC-based	AES	Signature	Blockchain	Moderate	Partial	No	Moderate	HC/HT domain absent; IoT only
SASE (Gartner model)	SSO/MFA	Policy-based	TLS/IPSEC	UEBA/IDS	Log analytics	Very High	Partial	High	High	Vendor proprietary; no HC-specific controls
XDR Platforms (commercial)	MFA+SSO	RBAC	At-rest+transit	XDR ensemble	SIEM	Very High	Partial	Partial	High	Black box; no ABE sharing; proprietary
Confidential Computing (TEE)	Attestation	Policy-TEE	In-use+rest	Audit TEE	Hardware	Low-Moderate	High	Moderate	Moderate	Hardware dependency; no IDS; emerging
Mishra et al. (2021) –	Token	IoT role	AES	Rule-based	Basic	Low	No	Yes	No	No HC; no ML IDS; no sharing protocol

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

Smart Hotel IoT										
Next-generation conceptual model (proposed)	Risk-adaptive MFA	Hybrid RBAC/ABAC	AES+ABE+PQC	ML+UEBA+FL	Merkle+ Blockchain	Cloud-native HPA	Full	Full	Full	Production validation; PQC maturity

Note. HC ✓ and HT ✓ indicate whether the architecture includes explicit design considerations for healthcare or hospitality contexts, respectively. 'Partial' indicates some domain consideration but not comprehensive coverage. The 'next-generation conceptual model' row represents the characteristics of an integrated architecture that the research community should pursue, as discussed in Section 7. HPA = Kubernetes Horizontal Pod Autoscaler.

The comparative analysis reveals three cross-cutting patterns of architectural inadequacy. First, a striking authentication-access control disconnection characterizes most research proposals: studies proposing sophisticated CP-ABE access control mechanisms (Li et al., 2013; Goyal et al., 2006) employ basic authentication without risk-adaptive calibration, while studies proposing sophisticated authentication mechanisms (Wazid et al., 2020) employ simple RBAC access control without ABAC expressiveness. No single architecture in the comparison matrix achieves excellence across both authentication and access control simultaneously, suggesting that the integration of these two layers has been treated as a secondary concern relative to the sophistication of each individual mechanism.

Second, the threat detection column reveals a fundamental division between architecture proposals that include comprehensive threat detection (IDS-focused studies like Singh et al., 2022 and Garg et al., 2020) and those that address threat detection not at all (most encryption and access control focused proposals). This absence of threat detection from architectures focused on other security dimensions reflects a theoretical gap: the principle of defence in depth requires that no single layer failure results in complete system compromise, which implies that all layers including threat detection must operate simultaneously. An architecture that provides excellent encryption and access control but no threat detection will fail to detect credential-based attacks in which an adversary uses legitimately obtained credentials to access data within the compromised account's authorized scope.

Third, the scalability column reveals a systematic underinvestment in evaluating security mechanisms under big data scale conditions. Twelve of fifteen architectures in the comparison receive 'Low' or 'Moderate' scalability ratings, reflecting either explicit acknowledgment of scalability limitations in the original publications or the absence of any scalability evaluation. Only commercial frameworks (SASE, XDR) and the proposed next-generation conceptual model achieve 'Very High' or 'Cloud-native HPA' scalability ratings a finding that underscores the urgency of scalability validation as a research priority for academic security proposals.

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025
IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business
UGC CARE II

6. Research Challenges

Table 7 characterizes nine research challenges that represent the current frontier of the cloud security field for healthcare and hospitality applications. The challenges span technical, organizational, and regulatory dimensions, reflecting the multi-disciplinary nature of the research problem.

Table 7: Research Challenges Matrix Technical, Organizational, and Regulatory Dimensions

Challenge	Technical Dimension	HC Manifestation	HT Manifestation	Severity	Maturity of Solutions
Cross-domain interoperability	No unified security API spanning HC, HT, tourism with consistent identity management	Hospital ↔ referral provider ↔ insurer sharing with incompatible identity schemes	Hotel ↔ OTA ↔ loyalty provider sharing with inconsistent API auth	Critical	FHIR provides HC standard; no HT equivalent
Big Data scalability of security	Encryption and access control overhead grows with data volume; IDS feature extraction at streaming scale	AES overhead on 500M patient record national EHR; DICOM bulk imaging encryption	Real-time fraud detection on 1M+ daily booking events	Critical	AES-NI accelerates AES; ML inference still bottleneck
Dynamic authorization	ABAC policy evaluation latency under concurrent peak access; attribute freshness; policy conflict detection	Emergency break-glass access must complete in < 2 seconds with full logging	Revenue manager seasonal role change must propagate immediately to all properties	High	OPA Rego + policy caching is partial solution
Cloud-native threat landscape	Container escape; serverless event injection; misconfiguration; supply chain; multi-tenancy side-channels	EHR cloud-native workload lateral movement	Cloud PMS injection via misconfigured Lambda	Critical	CSPM tools exist; integrated response lacking
Multi-cloud security consistency	Policy fragmentation across AWS/Azure/GCP; inconsistent IAM models; data residency enforcement	Hospital running EHR on AWS and imaging on Azure	Hotel chain with properties on multiple cloud providers	High	No open standard; SASE partially addresses

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

Privacy-utility trade-off	Differential privacy ε parameter: smaller ε → stronger privacy but lower analytical utility	Population health analytics under DP must remain clinically useful	Guest segmentation analytics under DP must remain commercially useful	High	Adaptive ε allocation is partial solution
Compliance complexity	Simultaneous HIPAA + GDPR + PCI DSS + national PDPA compliance in multi-jurisdiction deployments	Medical tourism: Indian patient data under ABDM + EU GDPR if European national	Multinational hotel: PCI DSS globally + GDPR in EU + PIPL in China	High	CCM v4 mapping helps; automated compliance still emerging
AI security and adversarial ML	IDS models vulnerable to adversarial examples; LLM-powered attacks; deepfake authentication bypass	Adversarial crafted network traffic evading clinical IDS	Deepfake-powered guest identity fraud	Emerging	Adversarial training; certified defences; XAI
Explainability and accountability	ML IDS black-box decisions are legally problematic for HIPAA adverse action notifications and GDPR Art. 22	Clinician access denied by ML policy must be explainable for HR process	Guest transaction declined must be explainable to avoid discrimination claims	High	SHAP/LIME exist; real-time integration limited
Resource-constrained endpoint security	IoMT devices and smart hotel room IoT lack processing power for standard TLS and MFA	Wearable cardiac monitor with 32KB RAM	Smart thermostat / room sensor with embedded MCU	High	DTLS; lightweight crypto; FIDO2 device attestation

Note. Challenge severity ratings (Critical, High, Emerging) reflect the combination of technical complexity and the documented operational impact of unresolved challenges in the existing literature. 'Maturity of Solutions' reflects the availability and deployment readiness of partial or complete technical solutions as of 2024.

6.1 The Cross-Domain Interoperability Challenge

The cross-domain interoperability challenge (C1) is arguably the most consequential research challenge for the field, because it determines the boundary conditions for any integrated security architecture. Healthcare data sharing today is mediated by HL7 FHIR R4 a mature, widely implemented standard that provides both a data model and an API specification for healthcare

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025
IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business
UGC CARE II

interoperability. Hospitality data sharing, by contrast, lacks an equivalent standard: OTA data exchange relies on proprietary implementations of OpenTravel Alliance (OTA) schemas and ad hoc REST APIs that differ substantially across technology vendors. The absence of a hospitality interoperability standard equivalent to FHIR creates specific challenges for security architectures that must provide consistent policy enforcement across heterogeneous API interfaces. Future research should develop or adapt a hospitality data interoperability standard that provides sufficient structure for meaningful access policy specification, analogous to the attribute and resource type definitions that FHIR provides for healthcare ABAC policy authoring.

6.2 Big Data Scalability of Security Mechanisms

The scalability challenge (C2) is both technically specific and practically consequential. AES-256-GCM encryption achieves throughputs exceeding 600 MB/s with AES-NI hardware acceleration sufficient for most individual healthcare and hospitality data processing workloads. However, the aggregate encryption throughput required for real-time processing of national-scale health data streams or large-scale hospitality analytics pipelines may exceed the capacity of individual encryption service instances, requiring horizontal scaling through multiple parallel encryption workers. The key management challenge amplifies this: each data object requires an individually managed DEK, and the key management service (AWS KMS, Azure Key Vault) becomes a potential bottleneck as the number of concurrent decryption requests scales with the number of concurrent data access operations. Future research should develop and benchmark hierarchical key management architectures specifically designed for big data workloads, with explicit measurement of key management service throughput under peak concurrent access conditions representative of national healthcare data exchange and large-scale hospitality analytics.

6.3 Compliance Complexity

The compliance complexity challenge (C7) reflects the intersection of multiple independent regulatory frameworks across multi-jurisdictional deployments that is increasingly common in both sectors. Healthcare organizations operating internationally must satisfy HIPAA Technical Safeguards for US patient data, GDPR Article 32 for EU patient data, India's DPDPA 2023 for Indian patient data, and potentially additional national healthcare data protection requirements in each country of operation simultaneously, with a single cloud infrastructure. Hospitality organizations operating globally face analogous multi-framework compliance obligations. The compliance complexity challenge is not primarily technical the technical controls required by different frameworks are often similar or identical but architectural: organizations need security architectures whose audit trails, access control logs, and data processing records can be efficiently mapped to the specific reporting requirements of multiple regulatory frameworks. Future research should develop compliance mapping frameworks that provide systematic mappings from security architecture components to the specific technical control requirements of all major applicable regulations, enabling automated compliance reporting from operational security telemetry.

7. Conceptual Future Research Roadmap

7.1 Architectural Principles for Next-Generation Integrated Security

The synthesis of the analytical findings from Sections 3 through 6 supports the development of a conceptual roadmap for next-generation integrated multi-layer cloud security architectures for

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

healthcare and hospitality. This roadmap is presented as a set of architectural principles and research requirements rather than a specific implementation, reflecting the review's objective of establishing the research agenda rather than proposing a specific solution.

Principle 1: Coordinated Layer Intelligence. Next-generation architectures must implement bidirectional security intelligence sharing among all security layers, enabling adaptive responses to emerging threats that integrate signals from multiple layers simultaneously. The authentication layer should consume threat detection signals to adjust factor requirements; the access control layer should consume risk scores from authentication and anomaly signals from threat detection; the audit layer should receive enriched, correlated events from all layers rather than independent event streams. This coordination requirement distinguishes truly integrated security architectures from collections of independent security tools deployed in the same environment.

Principle 2: Domain-Specific Calibration. Security mechanisms must be calibrated to the specific operational, regulatory, and threat characteristics of healthcare and hospitality deployments rather than applying generic enterprise security configurations. Authentication latency thresholds must reflect clinical workflow constraints identified in the healthcare informatics literature; ABAC policies must reflect the specific role structures and data sensitivity classifications of healthcare and hospitality organizations; IDS models must be trained on domain-specific attack patterns including insider EHR misuse, hospitality loyalty fraud, and medical device manipulation categories not represented in generic network benchmark datasets.

Principle 3: Cryptographic Enforcement. Security properties particularly access control and data sharing policies should be enforced at the cryptographic level wherever technically feasible, rather than relying exclusively on procedural or administrative controls that can be bypassed or misconfigured. CP-ABE policy embedding in ciphertext provides cryptographic enforcement of access policies for data sharing; authenticated encryption (AES-256-GCM) provides cryptographic enforcement of data integrity; and Merkle tree audit logging with digital signatures provides cryptographic non-repudiation for audit records. Cryptographic enforcement ensures that security properties are maintained even when administrative controls fail or are actively circumvented.

Principle 4: Algorithm Agility. Next-generation architectures must be designed for cryptographic algorithm substitution without requiring fundamental architectural redesign, accommodating the post-quantum migration that NIST's 2024 standardization of CRYSTALS-Kyber and CRYSTALS-Dilithium makes operationally urgent. Algorithm agility requires that specific cryptographic algorithms be configurable parameters in the architecture's algorithm registry rather than hard-coded dependencies, and that algorithm substitution be testable through dedicated test suites that verify security property preservation after algorithm change.

Principle 5: Privacy-Preserving Analytics by Default. Architectures should apply differential privacy and k-anonymity mechanisms to all analytical use cases as the default configuration, requiring explicit policy authorization for non-privacy-preserving analytics access rather than the reverse. This default application of privacy preservation reflects both the regulatory requirements of GDPR and HIPAA and the principle that the analytical value of healthcare and hospitality data should not require

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

compromising the privacy of the individuals whose data is being analyzed.

Principle 6: Empirical Validation at Production Scale. Next-generation architectures must be validated through cloud-deployed prototype evaluation at scale representative of production healthcare and hospitality deployments, not through simulation or small-scale academic testbeds. This validation requirement responds directly to the systematic prototype validation gap identified in the comparative literature analysis: proposals evaluated only through simulation cannot demonstrate the operational viability of their performance claims, leaving organizations without the empirical evidence needed to make informed deployment decisions.

7.2 Conceptual Architecture Dimensions

The conceptual next-generation integrated architecture should comprise, at minimum, eight coordinated security dimensions. The Adaptive Authentication dimension implements risk-adaptive multi-factor authentication with contextually calibrated factor requirements, FIDO2/WebAuthn phishing-resistant high-assurance factors, and UEBA-informed risk scoring that personalizes risk assessment to individual users' historical access patterns. The Hybrid Authorization dimension implements RBAC/ABAC hybrid access control with OPA/XACML policy evaluation, element-level data minimization, and purpose-based access control aligned to HIPAA minimum necessary and GDPR purpose limitation requirements. The Layered Encryption dimension implements AES-256-GCM at rest with hierarchical key management, TLS 1.3 in transit with certificate pinning, and CP-ABE for inter-organizational sharing with algorithm agility for post-quantum migration. The Secure Sharing dimension implements a cryptographically enforced sharing protocol verifying identity, attribute credentials, declared purpose, and data subject consent before any data is transmitted. The Continuous Monitoring dimension implements ML ensemble intrusion detection with LSTM sequential modeling, autoencoder anomaly detection, and UEBA individual baseline analytics, publishing security intelligence to a shared Security Orchestration Bus. The Privacy Preservation dimension applies differential privacy and k-anonymity to all analytical data products. The Auditability dimension implements SHA-3 Merkle-tree hash-chained audit logging with digital signature attribution and external tamper-evidence anchoring. The Scalability dimension implements containerized microservices with Kubernetes horizontal auto-scaling, ensuring that security processing capacity scales linearly with data volume without security property degradation.

8. Emerging Technologies and Their Security Implications

8.1 Artificial Intelligence and Explainable AI

The integration of large language models and foundation models into security operations security AI assistants, automated alert triage, natural language security policy authoring represents the most rapidly evolving development in cloud security practice. Security AI systems offer compelling operational advantages: the ability to query security logs in natural language ('Show me all access events by cardiologists to non-cardiac patient records in the last 30 days'), to automatically correlate alerts across multiple security layers into coherent incident narratives, and to generate remediation recommendations for common security misconfigurations. However, security AI systems introduce their own vulnerabilities: prompt injection attacks can manipulate AI-powered security tools; model hallucination can generate false security assurances; and the black-box nature of foundation model reasoning makes it difficult to audit AI-generated security decisions for regulatory accountability.

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025
IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business
UGC CARE II

Explainable AI (XAI) for intrusion detection applying SHAP (SHapley Additive exPlanations) or LIME (Local Interpretable Model-agnostic Explanations) to produce human-readable explanations of ML IDS classification decisions addresses the accountability gap in black-box ML security. XAI is particularly important in healthcare contexts where GDPR Article 22 and HIPAA adverse action notification requirements mandate that automated decisions affecting individuals be explainable. The research challenge is achieving real-time XAI generation: SHAP computation for a single prediction from a large ensemble model can require hundreds of milliseconds, which may be unacceptable for real-time intrusion detection scenarios. Research into computationally efficient XAI methods including approximate SHAP algorithms, attention-based explanations for deep learning models, and pre-computed SHAP value libraries for common attack patterns is needed to make XAI practical for production security operations.

8.2 Federated Learning for Distributed Security Intelligence

Federated learning (McMahan et al., 2017) enables the training of machine learning models across multiple distributed data sources without centralizing the raw training data each participating organization trains a local model update on its private data, and these updates are aggregated by a central server without the server ever seeing the raw data. Applied to intrusion detection, federated IDS enables multiple healthcare organizations or hotel chains to collectively train a superior threat detection model that reflects the diversity of attack patterns observed across all participating organizations, without any organization needing to share raw security event logs that may contain PHI or PII.

The primary security research challenge in federated IDS is gradient leakage: theoretical analysis has demonstrated that model gradients can, under certain conditions, be used to reconstruct training data samples (Geiping et al., 2020), potentially defeating the privacy objective of federated learning. Differential privacy applied to gradients adding calibrated noise to gradient updates before aggregation provides mathematical bounds on the privacy leakage risk but reduces model accuracy. The optimal privacy budget for federated IDS in healthcare and hospitality contexts the ε parameter that balances privacy protection with detection performance is an open research question requiring empirical evaluation in domain-specific settings.

8.3 Blockchain for Trust and Audit

Blockchain technology provides immutable, decentralized transaction ledgers that have two specific applications in healthcare and hospitality cloud security: tamper-evident audit logging and decentralized identity management. For audit logging, the publication of cryptographic Merkle root hashes to an external blockchain provides verifiable proof that the audit log has not been modified after publication, enabling regulatory auditors and data subjects to verify audit trail completeness without relying solely on the organization's self-reported records. For identity management, blockchain-based self-sovereign identity (SSI) systems in which individuals control their own identity credentials stored on a distributed ledger provide an alternative to centralized identity providers that eliminates the IdP single point of failure and enables privacy-preserving selective disclosure of identity attributes.

8.4 Digital Twins for Proactive Security

Digital twin technology the creation of continuously updated virtual replicas of physical systems that enable simulation and analysis without affecting the physical system has been applied to

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

industrial control system security (Eckhart & Ekelhart, 2018) and represents a promising direction for proactive cloud security simulation in healthcare and hospitality. A digital twin of a hospital's cloud security infrastructure would enable security teams to simulate attack scenarios testing whether a new ransomware variant would be detected by the current IDS model, or whether a new FHIR API endpoint is vulnerable to BOLA exploitation without risking the production environment. The research challenges include achieving sufficient fidelity of the digital twin to produce meaningful simulation results and developing the methodology for translating digital twin simulation findings into production security improvements.

9. Conclusion

This comprehensive review has critically evaluated the evolution of cloud security architectures, the current state and limitations of core security components, the adequacy of leading cloud security frameworks, and the research challenges that define the frontier of integrated cloud security for healthcare and hospitality systems. The review's central finding is that the current literature, despite its substantial volume and the sophistication of individual contributions, has not produced an integrated architectural framework that adequately addresses the complete security requirements of cloud-hosted healthcare and hospitality big data environments.The architectural deficiencies identified through the comparative analysis converge on a common root cause: the treatment of cloud security as a collection of independent mechanism problems rather than as an integrated coordination challenge. Encryption proposals do not address threat detection; IDS proposals do not address encryption or access control; access control proposals do not address secure data sharing. This mechanistic isolation prevents the emergence of the coordinated intelligence-sharing security properties that fundamentally differentiate truly integrated architectures from collections of independent tools. The Security Orchestration Bus concept in which bidirectional intelligence sharing among all security layers enables adaptive responses that no individual layer could achieve independently represents the architectural innovation that future research must develop, formalize, and empirically validate.The eight tables presented in this review provide systematic comparative evidence for the limitations of current approaches across authentication, access control, encryption, cloud security frameworks, threat detection, integrated architectures, research challenges, and future research priorities. The analysis consistently identifies scalability validation, cross-sector integration, and production-scale empirical evaluation as the three research priorities that would most substantially advance the field's ability to provide actionable security guidance to healthcare and hospitality organizations.

The future research agenda proposed in Section 7 and Table 8 identifies nine priority research directions, of which three are designated Critical: the design and empirical validation of an integrated cross-sector security architecture, post-quantum cryptography migration for long-lived healthcare and hospitality data, and large-scale production deployment studies. These three priorities share the property that their pursuit requires interdisciplinary collaboration spanning computer science, health informatics, hospitality management, cryptography, and privacy law that reflects the irreducibly multi-dimensional nature of the security problem. Research teams that can bridge these disciplines, combining the technical rigor of cryptographic security research with the operational understanding of healthcare and hospitality IT environments, are positioned to make the contributions that the field most urgently needs.

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

The convergence of increasingly sophisticated threats, expanding regulatory requirements, and rapidly growing cloud data environments in healthcare and hospitality creates both urgency and opportunity for the research agenda outlined in this review. The security of patient health information and guest personal data in cloud environments is not merely a technical problem it is a public health problem, a consumer protection problem, and increasingly a geopolitical problem as health data becomes a strategic asset in an era of state-sponsored cyber espionage. Research that advances the science of integrated cloud security for these sectors therefore has implications that extend well beyond academic contribution into the domain of meaningful societal benefit.

Table 8: Future Research Priorities A Nine-Direction Research Agenda

Research Priority	Addresses Challenge(s)	Priority Level	Time Horizon	Expected Breakthrough	Key Open Questions
Integrated cross-sector security architecture (HC+HT+Tourism)	C1, C2, C7	Critical	Near-term (1–3 yr)	First empirically validated framework eliminating domain fragmentation	Optimal layer coordination mechanism; Security Orchestration Bus design
Risk-adaptive authentication with clinical/HT calibration	C3	Critical	Near-term (1–2 yr)	MFA achieving both clinical workflow compatibility and phishing resistance	Optimal risk signal weighting for HC vs HT; cold-start problem
Post-quantum cryptography migration for HC/HT	C2, C6	Critical	Medium-term (2–5 yr)	Quantum-safe HC/HT cloud protecting 'harvest now decrypt later' threats	FIPS 203/204 performance in HC/HT big data contexts; migration sequencing
Federated IDS for multi-org HC/HT threat sharing	C1, C8	High	Near-term (2–4 yr)	Cross-organization threat intelligence without PHI/PII data sharing	Gradient leakage bounds; heterogeneous data distributions
Explainable AI for HC/HT security decisions	C9	High	Near-term (2–3 yr)	Real-time SHAP explanations for IDS alerts and access denials	Real-time XAI latency; explanation fidelity under adversarial conditions
Homomorphic encryption for clinical/guest analytics	C6	Medium	Medium-term (4–7 yr)	Computation on encrypted HC/HT data eliminating decryption risk	FHE performance for practical HC/HT query types; bootstrapping cost
Zero-trust IoMT/smart hotel security extension	C10	High	Near-term (1–3 yr)	Zero-trust micro-segmentation to resource-constrained IoT endpoints	Lightweight ZTA for 32KB MCU devices; device attestation at scale
Digital twin-based security simulation for HC/HT	C4	Medium	Medium-term (3–5 yr)	Proactive vulnerability discovery without production system risk	Digital twin fidelity requirements; attack simulation methodology
Production-scale HC/HT cloud security deployment studies	All	Critical	Medium-term (2–5 yr)	Enterprise-scale performance validation closing the prototype gap	Ethics frameworks; data governance; organizational adoption barriers

Note. Challenge codes refer to the challenges characterized in Table 7. 'Near-term' = 1–3 years; 'Medium-term' = 3–7 years. Priority designations reflect gap severity (from Table 7) combined with technical readiness of enabling technologies.

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

References

Abdulsalam, Y., & Hedabou, M. (2022). Security and privacy in cloud computing: Technical review. Future Internet, 14(1), Article 11. https://doi.org/10.3390/fi14010011

Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: Preserving security and privacy. Journal of Big Data, 5(1), 1–18. https://doi.org/10.1186/s40537-017-0110-7

Akinyele, J. A., Garman, C., Green, M., Hohenberger, S., Miers, I., Pagnia, P., Rubin, A. D., & Rupp, A. (2013). Charm: A framework for rapidly prototyping cryptosystems. Journal of Cryptographic Engineering, 3(2), 111–128. https://doi.org/10.1007/s13389-013-0057-3

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S. W., & Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. In Proceedings of the 13th EuroSys Conference (Article 30). https://doi.org/10.1145/3190508.3190538

Ayushman Bharat Digital Mission. (2023). ABDM operational guidelines 2023. Ministry of Health and Family Welfare, Government of India.

Bell, D. E., & LaPadula, L. J. (1973). Secure computer systems: Mathematical foundations. MITRE Corporation.

Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (pp. 321–334). https://doi.org/10.1109/SP.2007.11

Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In Proceedings of the 2012 IEEE Symposium on Security and Privacy (pp. 553–567). https://doi.org/10.1109/SP.2012.44

Buhalis, D., & Law, R. (2008). Progress in information technology and tourism management: 20 years on. Tourism Management, 29(4), 609–623. https://doi.org/10.1016/j.tourman.2008.01.005

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario.

Cheon, J. H., Kim, A., Kim, M., & Song, Y. (2017). Homomorphic encryption for arithmetic of approximate numbers. In Proceedings of ASIACRYPT 2017 (LNCS Vol. 10624, pp. 409–437). https://doi.org/10.1007/978-3-319-70694-8_15

Cloud Security Alliance. (2021). Cloud Controls Matrix v4. Cloud Security Alliance. https://cloudsecurityalliance.org/research/cloud-controls-matrix/

Confidential Computing Consortium. (2022). A technical analysis of confidential computing. Linux Foundation. https://confidentialcomputing.io/

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review. Maturitas, 113,

Copyright © 2025 | JVT Network, All Rights Reserved

Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 31, Issue 4 – Dec 2025

48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning. Future Generation Computer Systems, 82, 761–768. https://doi.org/10.1016/j.future.2017.08.043

Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3–4), 211–407. https://doi.org/10.1561/0400000042

Eckhart, M., & Ekelhart, A. (2018). A specification-based state replication approach for digital twins. In Proceedings of the CPS-SPC Workshop (pp. 36–47). ACM. https://doi.org/10.1145/3264888.3264892

European Parliament. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union.

Fan, J., & Vercauteren, F. (2012). Somewhat practical fully homomorphic encryption. IACR Cryptology ePrint Archive, 2012, 144.

Fernandez-Aleman, J. L., Carrion Señor, I., Lozoya, P. A. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, 46(3), 541–562. https://doi.org/10.1016/j.jbi.2012.12.003

Garg, S., Kaur, K., Kumar, N., Kaddoum, G., Zomaya, A. Y., & Ranjan, R. (2020). A hybrid deep learning-based model for anomaly detection in cloud datacenter networks. IEEE Transactions on Network and Service Management, 16(3), 924–935. https://doi.org/10.1109/TNSM.2019.2927886

Geiping, J., Bauermeister, H., Dröge, H., & Moeller, M. (2020). Inverting gradients: How easy is it to break privacy in federated learning? Advances in Neural Information Processing Systems, 33, 16937–16947.

Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM CCS (pp. 89–98). https://doi.org/10.1145/1180405.1180418

Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9(8), 1735–1780. https://doi.org/10.1162/neco.1997.9.8.1797

Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K., & Fen, A. (2013). Guide to attribute-based access control (ABAC) definition and considerations (NIST SP 800-162). NIST. https://doi.org/10.6028/NIST.SP.800-162

IBM Security. (2023). Cost of a data breach report 2023. IBM Corporation. https://www.ibm.com/reports/data-breach

Information Commissioner's Office. (2020). Marriott International Inc: Penalty notice. ICO UK.

Jiang, J., Chen, J., Dang, K., Lv, G., Li, K., & Ji, K. (2021). PFLF: Privacy-preserving federated learning framework for edge computing. IEEE Transactions on Information Forensics and

Copyright © 2025 | JVT Network, All Rights Reserved

Security, 16, 4656–4668. https://doi.org/10.1109/TIFS.2021.3110555

Kindervag, J. (2010). No more chewy centres: Introducing the Zero Trust model of information security. Forrester Research.

Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation, 48(177), 203–209. https://doi.org/10.1090/S0025-5718-1987-0866109-5

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review. Technology and Health Care, 25(1), 1–10. https://doi.org/10.3233/THC-161263

Kumari, P., Tanwar, S., Tyagi, S., & Kumar, N. (2023). Federated learning for data analytics in healthcare. IEEE Internet of Things Journal, 10(4), 2865–2879. https://doi.org/10.1109/JIOT.2022.3228511

Kwon, J., & Johnson, M. E. (2021). Investigating the association between hospital ransomware attacks and patient outcomes. JAMA, 325(18), 1892–1899. https://doi.org/10.1001/jama.2021.4390

Lee, A. (2019). Your Pa$$word doesn't matter. Microsoft Security Blog.

Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and secure sharing of personal health records in cloud using ABE. IEEE Transactions on Parallel and Distributed Systems, 24(1), 131–143. https://doi.org/10.1109/TPDS.2012.97

Lundberg, S. M., & Lee, S. I. (2017). A unified approach to interpreting model predictions. Advances in Neural Information Processing Systems, 30, 4765–4774.

McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Agüera y Arcas, B. (2017). Communication-efficient learning of deep networks from decentralized data. In Proceedings of AISTATS 2017 (Vol. 54, pp. 1273–1282). PMLR.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (NIST SP 800-145). NIST. https://doi.org/10.6028/NIST.SP.800-145

Mishra, N., Lin, C. C., & Chang, H. T. (2021). A cognitive adopted framework for IoT big-data management. International Journal of Distributed Sensor Networks, 11, Article 718483.

MITRE. (2023). ATT&CK for cloud. MITRE Corporation. https://attack.mitre.org/matrices/enterprise/cloud/

Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection. In Proceedings of MilCIS. IEEE. https://doi.org/10.1109/MilCIS.2015.7348942

Nair, M. M., & Patil, V. (2023). Differential privacy for machine learning on electronic health records. International Journal of Advanced Computer Science and Applications, 14(3), 123–132.

NIST. (2017). Digital identity guidelines (NIST SP 800-63B). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b

NIST. (2018). Framework for improving critical infrastructure cybersecurity v1.1. NIST.

Copyright © 2025 | JVT Network, All Rights Reserved

NIST. (2024). FIPS 203: Module-lattice-based key-encapsulation mechanism standard. NIST. https://doi.org/10.6028/NIST.FIPS.203

NIST. (2024). FIPS 204: Module-lattice-based digital signature standard. NIST. https://doi.org/10.6028/NIST.FIPS.204

OWASP. (2023). OWASP API security top 10: 2023. Open Web Application Security Project. https://owasp.org/API-Security/

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45–77.

Rathore, S., Park, J. H., & Chang, H. (2021). Deep learning and blockchain-empowered security for 5G IoT. IEEE Internet of Things Journal, 8(18), 14364–14379. https://doi.org/10.1109/JIOT.2020.3043939

Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). 'Why should I trust you?': Explaining the predictions of any classifier. In Proceedings of KDD 2016 (pp. 1135–1144). https://doi.org/10.1145/2939672.2939778

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126. https://doi.org/10.1145/359340.359342

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST SP 800-207). NIST. https://doi.org/10.6028/NIST.SP.800-207

Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. In Proceedings of EUROCRYPT 2005 (LNCS Vol. 3494, pp. 457–473). Springer.

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. Proceedings of the IEEE, 63(9), 1278–1308. https://doi.org/10.1109/PROC.1975.9939

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. IEEE Computer, 29(2), 38–47. https://doi.org/10.1109/2.485845

Singh, J., Silakari, S., & Soni, G. (2022). A novel deep learning architecture for intrusion detection in cloud computing. International Journal of Advanced Computer Science and Applications, 13(7), 457–468.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (pp. 124–134). IEEE.

Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. In Proceedings of the 22nd

Copyright © 2025 | JVT Network, All Rights Reserved

ACM SIGSAC CCS (pp. 1310–1321). https://doi.org/10.1145/2810103.2813687

Sophos. (2023). The state of ransomware in healthcare 2023. Sophos Ltd.

Srivastava, A., Srivastava, S., & Srivastava, P. (2023). Data governance in hospitality and tourism. Journal of Hospitality and Tourism Technology, 14(2), 178–197.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1–11. https://doi.org/10.1016/j.jnca.2010.07.006

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In Proceedings of CISDA (pp. 1–6). IEEE.

Verizon. (2023). 2023 data breach investigations report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

W3C. (2021). Web authentication: An API for accessing public key credentials level 2. W3C Recommendation. https://www.w3.org/TR/webauthn-2/

Wazid, M., Das, A. K., Bhat, K. V., & Vasilakos, A. V. (2020). LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. Journal of Network and Computer Applications, 150, Article 102496. https://doi.org/10.1016/j.jnca.2019.102496

Yang, X., Yi, X., Nepal, S., Kelarev, A., & Han, F. (2020). Blockchain-based secure and lightweight authentication for IoT. IEEE Internet of Things Journal, 7(10), 9587–9598. https://doi.org/10.1109/JIOT.2020.2993784

Zhang, J., Chen, B., Zhao, Y., Cheng, X., & Hu, F. (2021). Data security and privacy-preserving in edge computing paradigm. IEEE Access, 6, 18209–18237. https://doi.org/10.1109/ACCESS.2018.2820162

Copyright © 2025 | JVT Network, All Rights Reserved