Quantum Key Distribution and Hybrid Quantum–Classical Cryptography for Secure Cloud Storage a Critical Review

Ibrahim Manga*, Barka Mshelia Sunday, and Omega Sarjiyus

Department of Computer Science, Adamawa State University, Mubi, Nigeria

***Corresponding Author**

DOI: https://doi.org/10.51584/IJRIAS.2026.11100072

Received: 18 October 2026; Accepted: 23 October 2026; Published: 10 November 2026

ABSTRACT

Protecting cloud-stored information against quantum-era threats requires more than selecting a key-establishment mechanism. Quantum key distribution (QKD) must operate alongside authenticated classical communication, secure key delivery, reliable endpoints, and appropriate data encryption. This critical narrative review examines how these dependencies are represented in QKD and hybrid quantum–classical security research. The synthesis draws on targeted literature searches, primary publisher and institutional records, reference-list tracing, and official standards and agency publications. Thirty sources were retained, including fourteen studies mapped comparatively. Full-text consultation is distinguished from abstract or record-only access, and no systematic completeness or independent dual screening is claimed. The analysis uses three consistent research questions concerning mechanism integration, demonstrated security and performance, and deployment requirements. The synthesis identifies four distinct integration purposes: classical-channel authentication, combination of independent key sources, protocol-level efficiency enhancement, and application-facing key delivery. Optical authentication experiments, hardware prototypes, formal hybrid protocols, and deployed-network benchmarks provide stronger integration evidence than an interpretation based only on simulated disturbance. Nevertheless, these contributions do not independently demonstrate authenticated cloud-object storage and recovery across all relevant threats. A security-assumption taxonomy separates device, authentication, key-processing, combiner, delivery, endpoint, and availability dependencies. The comparative mapping records authentication, implementation setting, security measures, metrics, access status, and evidence type. ETSI interfaces and national security agency guidance expose further operational constraints, while a disclosed coauthored study is assessed using the same criteria as other sources. The review concludes with staged evaluation requirements linking key establishment to authenticated object retrieval. No new cryptographic protocol, implementation, or experimental result is claimed.

Keywords: Quantum key distribution, post-quantum cryptography, cloud storage security, authentication, key management

INTRODUCTION

Cloud-storage confidentiality depends on the relationship between data encryption, key establishment, access control, and endpoint operation. An attacker may record encrypted communications for future decryption, steal an application key, impersonate a key service, or alter an object's metadata. A change to the key-establishment layer addresses only part of this threat surface. Consequently, quantum-era storage protection must be assessed as an operational workflow rather than as a property inherited from a single cryptographic component [4, 16].

QKD and post-quantum cryptography (PQC) address different assumptions. QKD distributes correlated secret material using quantum communication and authenticated public discussion. PQC uses classical algorithms built on mathematical problems believed to resist quantum attacks. Foundational reviews explain both the theoretical opportunities and the practical device assumptions involved in QKD [18, 30]. This article considers their integration into cloud-security services without treating physical key distribution, simulated quantum circuits, and classical post-quantum algorithms as interchangeable.

The synthesis extends beyond disturbance-based BB84 studies to include authentication experiments, hybrid authenticated key exchange, TLS and MACsec integration, key-delivery interfaces, and agency deployment guidance. Its contributions are a comparative evidence map, an explicit security-assumption taxonomy, and an evaluation framework that connects protocol evidence to cloud-object protection. These are analytical contributions; the review does not introduce or experimentally validate a new cryptographic construction.

Research questions

RQ1: How are QKD and PQC integrated for authentication, key combination, protocol operation, and delivery of keys to cloud-facing applications?

RQ2: What security properties and performance outcomes are supported by the accessible evidence, and under which implementation and trust assumptions?

RQ3: Which additional requirements must be evaluated before protocol or network results support claims about secure cloud-object storage and recovery?

METHODOLOGY

Review design and information sources

This study is a critical narrative review intended to explain security assumptions and assess the transfer of protocol evidence to cloud storage. This design accommodates analytical papers, simulations, optical experiments, standards, and policy guidance whose outcomes cannot be pooled meaningfully. Targeted web searches located primary publisher records, institutional repositories, author-hosted manuscripts, and official standards and agency publications. Reference-list tracing identified further relevant work, while exact-title and DOI searches corroborated bibliographic identity and helped locate accessible texts. Appendix A provides the core search expressions. The method supports transparent inspection of source selection; it is not an exhaustive systematic review.

Recent QKD and PQC integration studies were emphasized, while foundational and normative sources were retained where necessary to interpret authentication, BB84, finite-key analysis, authenticated encryption, and key derivation. Information was accessed through IEEE and other publisher records, Springer Nature Link, Wiley, MDPI, institutional repositories, arXiv versions linked to published works, ETSI, NIST, the RFC Editor, NSA, and NCSC. These are access routes; the review does not claim that subscription databases such as Scopus or Web of Science were searched.

Eligibility and source handling

A source was retained if it specified a QKD/PQC mechanism relevant to authentication or cloud-facing key management, analyzed QKD security assumptions, reported an integration or performance evaluation, or supplied directly relevant standards or deployment guidance. Generic quantum-computing commentary, unrelated application demonstrations, duplicate versions of the same work, and unsupported descriptions without an identifiable primary record were excluded from substantive evidence. Lossless compression was not an appraisal criterion because it does not directly answer the research questions.

The source set was assembled purposively from candidate references, targeted searches, and reference-list tracing. Relevance was assessed against the three research questions and the eligibility criteria above. Records were matched by DOI where available and otherwise by title, authors, and venue; publisher and institutional versions of the same work were treated as one source. Thirty sources were retained: fourteen studies for comparative appraisal and sixteen foundational, standards, or guidance sources for interpretation. These figures describe the final corpus. A complete record of all retrieved and excluded candidates was not retained, so screening totals, exclusion frequencies, and a PRISMA flow are not reported. Appendix B identifies the consulted source and access level for each retained reference.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue X October 2026

FT denotes consultation of full-text sections relevant to the extracted claims; AR denotes abstract, bibliographic-record, official landing-page, or bibliographic-front-matter access. The corpus contains 21 FT and 9 AR sources. Where an author manuscript was consulted, its published bibliographic identity was checked separately. AR sources support limited descriptive statements and are not used to infer unseen authentication or implementation details. For FT sources, an unestablished detail refers to the inspected sections; for AR sources, "not assessable" identifies an access limitation. Neither classification implies complete reading of every article, independent dual assessment, proof verification, or experimental replication.

Extraction and evidence classification

Each comparative study was assessed for integration purpose, authentication and initial trust, simulated or optical setting, stated security measures, reported metrics, evidence type, and transfer limits. The same fields were used throughout Table 1. Evidence types are analytical/protocol reasoning (AN), software or circuit simulation (SIM), laboratory or controlled testbed evaluation (LAB), and deployed-network evaluation (DEP). A work may have more than one type. This classification describes what was studied; it is not a numerical quality ranking or a replacement for a formal risk-of-bias instrument. RQ1 is answered through the integration, authentication, and key-delivery fields; RQ2 through implementation setting, security measures, reported metrics, and evidence type; RQ3 through inference boundaries, the assumption taxonomy, and the staged application tests. Missing authentication details are not imputed from the presence of PQC or QKD.

Extraction and editorial organization were AI-assisted. No preregistered protocol, independent dual screening, or statistical meta-analysis was performed. Bibliographic details were checked afresh against external publisher, institutional, author-hosted, archive, or official issuing-body records, rather than accepted solely from AI-generated citations. Those checks corroborate publication identity and citation details; they do not establish independent human verification of the findings. The search expressions, eligibility criteria, comparison fields, and source-access register improve methodological transparency and allow readers to inspect the basis of the synthesis. They do not establish full search reproducibility or systematic completeness.

Coauthored evidence and appraisal safeguards

Omega Sarjiyus, a coauthor of this review, also coauthored the cloud-security study cited as Sarjiyus et al. [23]. That overlap is disclosed here and in the declarations. The study receives no privileged evidence status: its implementation claims, authentication description, metrics, and reporting limitations are assessed using the same fields as all other sources. The review does not claim an independent external assessment of that work.

RESULTS AND CRITICAL SYNTHESIS

Comparative evidence map

Table 1 maps fourteen studies to the research questions. Its implementation and authentication columns prevent a physical optical experiment from being equated with a circuit simulation or an incompletely described cloud architecture. FT/AR records the access used for this review. Numerical results remain attributed to each study and are not pooled or ranked across unlike workloads. All observations in the table are a synthesis of published reports rather than measurements made for this review.

Table 1 Comparative evidence on authentication integration and deployment limits

Study	Setting and access	Authentication and initial trust	Security mechanism	Reported metrics	Evidence	Boundary of inference
Wang et al. [28]	Optical QKD networks; FT	Aigis-Sig certificates; trusted CA and	PQC-signed classical messages; replay nonces	Authentication operation, QBER and key rates	LAB	Evidence for channel authentication; not a stored-object recovery test.

		provisioned CA public key				
Garms et al. [8]	Optical prototype and FPGA; FT	PSK with MAC or classical/PQ signatures; provisioned credentials	Muckle++ hybrid exchange and evolving secret state	Hardware operation and hybrid key processing	AN + LAB	Security depends on the instantiated authentication and key-combination mode.
Rubio García et al. [21]	TLS implementation reported; AR	Detailed trust provisioning not assessable from consulted abstract	QKD/PQC concatenation and XOR approaches	Study-specific TLS handshake comparisons	LAB reported	Full implementation details not rechecked; no cloud-object claim inferred.
Buruaga et al. 2025 [3]	MACsec protocol integration; FT	PSKs, PQ signatures, or both; PSK/PKI provisioning	VMuckle supplies root key to MACsec key agreement	Protocol analysis and communication/performance costs	AN + integration	Data-link protection does not independently establish storage-at-rest protection.
Buruaga et al. 2026 [2]	MadQCI optical network; FT	ML-DSA-65 selected for the evaluated setup; PKI trust	Hybrid TLS using key export interfaces	Handshake latency across direct/relayed topologies	DEP	Real network evidence; not a complete object-store lifecycle benchmark.
Maned et al. [12]	BBM protocol analysis; FT	Public-key authenticity required; basis encryption is not identity authentication	McEliece-based encrypted bases with QKD	Modeled key-rate improvement around 2×	AN	Protocol-rate claim; separate deployment, authentication and fallback analysis needed.
Sarjiyus et al. [23]	Claimed optical/private-cloud testbed; FT	Dilithium signatures in PQC mode; QKD-only uses PSK-style TLS	Kyber/QKD XOR combination reported	Handshake latency, transfer throughput and key rate	LAB reported	Coauthored source; mixed tense and missing trace artifacts limit independent verification.
Prathyusha et al. [20]	Multi-cloud with emulated QKD; FT	Initial classical-channel authentication not established in inspected methods	Lattice-based scheme, BB84 component and slicing	Encryption time, throughput, entropy and avalanche	SIM / software evaluation	Emulation is not optical validation; randomness metrics do not prove secrecy.
Singamaneni et al. [24]	Multi-qubit cloud model; FT	Access-policy model; QKD bootstrap authentication not established	QKD combined with CP-ABE	Model security/performance comparisons	SIM	Access control and QKD source authentication require distinct assessment.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue X October 2026

Kim et al. [9]	Eight compute nodes; BB84 Qiskit Aer simulation; FT	Signatures discussed as an addition; deployed bootstrap not established in inspected implementation	Kyber512; simulated QKD masking of PQC secret key; parallel AES	Reported 2.37× overall and 8.11× encryption speedups	SIM + software benchmark	No optical QKD measurement; parallelism prevents attribution of speedup to QKD alone.
Fiorini et al. [7]	Noisy BB84 simulator; AR	Not assessable at abstract/record access	Interception-density estimation under noise	QBER and interception-density estimation	SIM	Protocol inference study, not authenticated cloud storage.
Lee et al. [11]	Analytical and simulation study; AR	Not assessable at abstract/record access	Threshold/grouped BB84 detection analysis	False-positive and false-negative behavior	AN + SIM	Detection accuracy is not final-key secrecy.
Ul Ain et al. [27]	BB84/E91 circuit models; FT	Authenticated public channel discussed; bootstrap provisioning not established	Basis/qubit configurations and error mitigation	Protocol and modeled interception outcomes	SIM	Circuit behavior does not establish an optical or cloud deployment.
Smiles and Sevugarajan [25]	Qiskit/IoT/cloud implementation reported; AR	Not assessable at publisher-abstract access	BB84, ASCON and blockchain-related integrity	QBER, encryption and verification timing	SIM/integration reported	Physical link and finite-key processing cannot be established from the abstract.

AN = analytical/protocol; SIM = simulation; LAB = controlled testbed; DEP = deployed network. FT = full-text sections consulted; AR = abstract/record only. “Reported” preserves attribution and does not mean independently reproduced. Source: review synthesis of the cited publications.

Authentication and integrated network evidence

Wang et al. [28] demonstrate PQC authentication of optical QKD using certificates and a trusted certification authority. The consulted author manuscript specifies Aigis-Sig, replay nonces, and authenticated processing messages. This supports the feasibility of replacing extensive pairwise secret distribution with PKI-based trust, but it is not evidence that authentication can start without a trust anchor. Nor should this historical Aigis-Sig implementation be described as an ML-DSA implementation.

Garms et al. [8] develop Muckle++ and demonstrate it on an optical QKD prototype with FPGA-based processing. Their architecture distinguishes PSK/MAC authentication from authentication with classical and post-quantum signatures. The security obtained depends on that choice; a signature-based configuration must not be assigned information-theoretic authentication simply because QKD is also present. This distinction is central when translating a hybrid construction into a cloud service.

VMuckle extends the protocol discussion to MACsec and permits PSK, post-quantum-signature, or combined authentication [3]. The later MadQCI benchmark evaluates hybrid TLS on actual optical infrastructure, including direct and trusted-relay topologies and application-facing key export [2]. These sources correct any suggestion

that all relevant work is simulation-only. Their results concern channel and network integration; storage authorization, object versioning, retention, and authenticated recovery remain additional application obligations.

Rubio García et al. [21] report TLS implementations combining QKD and PQC through concatenation and XOR. Their accessible abstract supports an integration and handshake-performance claim, but the full implementation was not available for this review. Detailed claims about their credential provisioning are therefore withheld. The study is retained as limited-access evidence rather than being silently treated as fully assessed.

Cloud-oriented architectures and corrected classifications

The Prathyusha et al. framework explicitly includes a QKD component, so it should not be relabeled as purely PQC. However, its methods describe an emulated QKD evaluation [20]. The appropriate classification is a lattice/QKD multi-cloud proposal with software evaluation, not a verified optical deployment. Reported entropy and avalanche indicators cannot by themselves certify authentication, finite-key secrecy, or resistance to quantum cryptanalysis.

Singamaneni et al. combine a multi-qubit QKD model with ciphertext-policy attribute-based encryption [24]. This addresses a different question from authenticating the origin of QKD messages: an access policy governs who may decrypt, while the QKD bootstrap must establish whom the participants are communicating with. The inspected description does not establish that the latter follows automatically from the former.

Kim et al. [9] implement distributed file partitioning and parallel AES on an eight-node compute cluster, while the BB84 key component is emulated in Qiskit Aer (Sections 2.2, 3.4 and 4.1). Their implementation uses Kyber512 and describes XOR masking of the PQC secret key with the simulated QKD session key. This is software integration with simulated QKD, not an optical QKD experiment. The paper discusses adding signatures, but the inspected implementation does not establish deployed classical-channel authentication. Its limitations section also explicitly acknowledges the absence of cryptographic integrity verification for encrypted subsets and keys. The reported 2.37× overall and 8.11× encryption speedups cannot isolate a QKD benefit without a matched architectural ablation.

Sarjiyus et al. report a private-cloud arrangement and a 50-km optical QKD setup, with signatures and an XOR key combination [23]. The paper supplies latency and throughput tables, but the setup also mixes completed and prospective wording. This review therefore records a reported laboratory evaluation rather than independently verified deployment. The lack of accessible measurement traces and a sufficiently explicit hybrid security argument restricts reproducibility. The coauthor relationship does not remove these limitations.

Protocol observations and the limits of disturbance metrics

BB84 uses incompatible preparation and measurement bases and subsequent classical processing [1]. A QBER observation characterizes disagreement in a defined sample; its interpretation depends on the channel, device model, interception model, and sample size. The detection-focused work of Lee et al., Fiorini et al., and Ul Ain et al. addresses analytical or simulated protocol behavior [7, 11, 27]. Smiles and Sevugarajan describe a broader BB84/ASCON/cloud pipeline at publisher-abstract access [25]. None of these descriptions alone establishes a composable end-to-end storage guarantee.

Finite-key analysis links observed parameters to a bound on extractable secret material under stated assumptions [26]. Sifted bits, disclosed test bits, reconciled bits, and final secret bits should therefore be counted separately. An illustrative 11% rejection rule is not a universal security theorem. A QBER alarm also does not uniquely identify an attacker because benign noise and device errors can contribute to disturbance. Security claims must state the applicable protocol, adversary, finite-size treatment, and failure parameters [19, 30].

Statistical randomness testing is diagnostic rather than a proof of key secrecy. Passing a test suite cannot establish that an adversary lacks the generator state or correlated side information; NIST explicitly limits what such tests can establish [22]. Similarly, a key-derivation function can extract or expand suitable input material under its assumptions but cannot manufacture secret entropy from public or compromised bits [10]. These distinctions

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue X October 2026

prevent entropy scores, apparent randomness, or HKDF output length from being substituted for a key-security analysis.

Security-assumption taxonomy

Table 2 makes explicit the taxonomy promised in the abstract. It is an analytical coding framework for the reviewed evidence, not a new proof of security. A claim should identify which assumptions apply and what fails when one is removed. The categories separate mechanisms that are often grouped under a single "quantum-secure" label. Their relevance follows from QKD security analysis, authenticated exchange, and application-interface requirements [5, 6, 13, 19].

Table 2 Taxonomy of assumptions requiring separate evidence

Assumption category	Required specification	Appraisal question
Quantum devices and channel	Source/detector models, loss, noise, calibration and side channels	Does the claimed security model match the actual equipment or simulator?
Classical authentication and initial trust	Provisioned PSK or authenticated public-key/CA roots	Can an active adversary replace peers, credentials or protocol messages?
Secret-key processing	Parameter estimation, reconciliation leakage, privacy amplification, finite-size failure bounds	Is the measured quantity a sifted count or a justified final secret length?
Hybrid combination and binding	Combiner assumptions, component independence, identities and transcript binding	Does the claimed resilience survive the specified component compromise?
Key delivery and service boundary	Authenticated key-manager interface, key identifiers and authorization	Can the right application obtain the right key without exposing another tenant's key?
Endpoint and stored-key trust	Memory, hardware boundary, backups, access control, erasure and rotation	What remains protected after endpoint or key-store compromise?
Object protection and recovery	AEAD configuration, nonce uniqueness, authenticated metadata and version checks	Are tampering, rollback and wrong-key retrieval rejected before plaintext release?
Availability and fallback	Key-pool exhaustion, optical failure, relay trust and downgrade policy	Does a failure cause an explicit abort or an authorized, authenticated fallback?

DISCUSSION

Classical-channel authentication and initial trust

QKD does not authenticate a peer solely by detecting disturbance. Two independently established QKD sessions can be made to terminate at an impersonator unless the classical exchanges are authenticated. The bootstrap must therefore begin with trusted material established outside the first unauthenticated QKD exchange. A deployment can provision a high-entropy symmetric authentication secret through a controlled channel, or install authenticated public keys and a trusted certification-authority root. QKD cannot retroactively authenticate its own initial session.

A universal-hash message-authentication construction can authenticate public messages using shared secret material [29]. Its security depends on the actual construction, tag policy, message limits, and correct treatment of consumed or reusable key components. A design should budget authentication material and, after a successful authenticated QKD session, reserve appropriate fresh secret bits for future use. An abort must not be assumed to replenish that budget. This is key expansion from established trust, not key establishment without initial trust.

With PQC signatures, each endpoint instead requires a securely bound verification key or certificate, protected signing keys, credential validation, and replay-resistant transcript processing. ML-DSA is a signature standard, whereas ML-KEM establishes shared material and does not alone authenticate an identity [15, 16]. A KEM can participate in an authenticated construction, but a bare encapsulation to an unauthenticated public key does not solve impersonation. Mosca et al. analyze why computational authentication that holds during protocol execution can be compatible with long-term QKD secrecy in the stated model [13]; that is narrower than claiming unconditional security of the entire application.

Hybrid combination and security boundaries

Authentication, secret combination, and storage encryption should be described as separate protocol decisions. An XOR of two equal-length values can preserve secrecy under suitable assumptions, but naming XOR does not establish independence, freshness, correct peer binding, or resistance to active substitution. Concatenation followed by a KDF likewise needs a defined security model and input handling. Reviewed hybrid constructions are valuable because they articulate some of these dependencies, rather than merely placing algorithm names in an architecture [3, 8, 21].

Maned et al. use McEliece-based encryption of basis information to modify BB84 operation [12]. Their approximately twofold rate claim concerns the proposed protocol's accounting, not a measurement of cloud-object throughput. Their fallback also changes the source of security when no distilled QKD key is available. A deployment must make that change explicit and authenticate the negotiated mode. The label used for a code-based primitive should not be assumed to identify the exact parameters or security properties of another implementation.

These distinctions are also relevant to the payload cipher. A quantum-origin key used with AES-GCM still yields a computational authenticated-encryption service, rather than information-theoretic message confidentiality. The security of the key supplier and the security of the data cipher are related but different claims. The application must use the selected cipher within its specified nonce, tag, message-length, and usage limits [4].

ETSI interfaces and delivery to cloud applications

ETSI GS QKD 004 V2.1.1 specifies an interface between a QKD key manager and applications, including session-oriented key access and quality-of-service concepts [6]. It helps define the boundary at which a cryptographic application obtains matching key material. That interface is distinct from the optical protocol and does not by itself prove that the source devices or the application are secure.

ETSI GS QKD 014 V1.1.1 specifies HTTPS/JSON delivery of block keys and identifiers [5]. Applications request keys from local key-management entities, and a peer can retrieve corresponding material using the identifiers. The specification requires mutual certificate authentication at the application–manager connection and leaves certificate installation or upgrading outside its scope. Consequently, interface compliance does not resolve certificate bootstrap, quantum-safe credential migration, key-store compromise, or authorization of a specific cloud tenant.

A proposed storage integration should bind the key identifier to the authorized object and version, separate tenants' key namespaces, prevent duplicate consumption, and define behavior when a peer requests an unknown key or the pool is empty. These are review-derived engineering requirements. They must be tested in the actual adapter or key service rather than inferred from compliance with a key-delivery message format. Secure optical generation is insufficient if a delivery endpoint releases the material to the wrong application.

National security agency positions and their scope

The US NSA identifies source-authentication dependencies, specialized equipment, trusted-relay exposure, implementation assurance, and denial-of-service risk as obstacles to using QKD in National Security Systems [17]. Its position favors post-quantum cryptography for that mission unless the stated limitations are overcome. This is deployment guidance for a defined institutional security context, not a proof that every QKD experiment is invalid or a rule automatically binding every civilian cloud service.

The UK NCSC's quantum-security guidance does not endorse QKD for government or military applications and cautions against relying on it alone for business-critical networks [14]. It emphasizes quantum-safe authentication alongside any QKD use. These positions are included as operational counterweights to optimistic integration papers. They should be read together with, rather than used to erase, published optical and network demonstrations. Demonstrating a functioning system and meeting an organization's assurance, cost, and maintainability requirements are different outcomes.

What the evidence does and does not establish

The expanded corpus establishes that relevant hybrid research includes physical systems and network integration, not only simulation. It supports feasibility claims for particular authentication and key-exchange designs. It does not justify a universal performance ranking, a blanket statement that hybridization is always beneficial, or a claim that production cloud-object security follows from a successful handshake. A missing detail is recorded as an uncertainty in accessible reporting; it is not evidence that the original implementation necessarily omitted the feature.

Evidence transfer should follow the tested boundary. A network experiment can inform handshake and key-delivery cost. A storage experiment can establish rejection of a corrupted object under stated conditions. A formal protocol proof can establish security within a model. Those results become an end-to-end assurance argument only when the trust assumptions align and the composition is justified. The specific research gap is therefore the need for better-connected, reproducible evidence across these boundaries within the reviewed corpus, not an assertion that no integrated work exists.

Practical Evaluation Framework

Stage one protocol and authentication verification

Specify the protocol version, device or simulator, adversary, credentials, trust anchors, and security parameters before benchmarking. Test peer impersonation, invalid or revoked credentials, message modification, replay, mismatched transcripts, and authentication failure. Distinguish a model with trusted public discussion from an implementation that actually authenticates it. For QKD, record raw, sampled, sifted, reconciled, and final key lengths and the relevant leakage and finite-key assumptions. The framework is a proposed evaluation procedure, not an experiment completed for this review.

Stage two key-service and cloud-object integration

Evaluate authorized key delivery independently from generation. Test wrong key identifiers, cross-tenant requests, stale credentials, duplicate consumption, pool depletion, and manager unavailability. Then test object encryption and retrieval with explicit associated data, object versions, nonce management, rotation, and retention policies. Reject altered ciphertext or tags, wrong keys, and unauthorized object versions before releasing plaintext or passing it to another processing stage. Record successful authenticated recovery and exact file equality separately from merely returning a response.

Stage three matched comparison and fault reporting

Use matched files, hardware, payload cipher, authentication level, and network conditions across an authenticated classical comparator, an authenticated standardized PQC comparator, and a hybrid configuration. Where feasible, isolate the key supplier while keeping the storage pipeline unchanged. Report handshake and

retrieval latency distributions, communication bytes, CPU, memory, final-key availability, rejection counts, object overhead, and recovery outcomes. Include both successful and failed sessions in availability analysis, and identify whether timing excludes retries, key pre-generation, or recovery operations.

Separate first-session provisioning, steady-state operation, rotation, and failure recovery. A prefilled key pool can reduce apparent handshake cost without eliminating the earlier generation and distribution expense. Likewise, parallel file encryption can dominate overall speedup. Compare physical and simulated configurations in separate result groups and avoid extrapolating a small testbed directly to a multi-provider service. Report raw measurements and configuration artifacts sufficient to inspect the claimed effect; do not interpret an entropy score or a single best-case timing as a general assurance result.

Limitations

The review uses purposive selection and targeted, AI-assisted retrieval rather than an exhaustive systematic search. Search-engine rankings change, and a complete record of all candidate records and exclusion decisions is unavailable; consequently, the precise selection process cannot be reconstructed in full. The search expressions and source-access register improve transparency without removing this limitation. Access barriers restrict some studies, including the TLS article, to descriptive AR evidence. Bibliographic identities were checked externally, but findings, proofs, and experiments were not independently validated or reproduced, and no independent dual screening was performed. The corpus overrepresents accessible English-language sources. The taxonomy is an analytical framework rather than a validated quality score. Disclosed coauthor overlap in one reviewed study introduces possible interpretive bias, addressed through the same appraisal fields used for other sources. The conclusions therefore apply to the selected evidence and do not establish systematic completeness or universal comparative superiority.

CONCLUSION

This critical review distinguishes authentication of QKD messages, hybrid key combination, protocol-level modifications, and application-facing key delivery. The expanded evidence includes optical experiments, hardware prototypes, formal protocol work, and deployed-network evaluation, alongside simulated and limited-access cloud proposals. The explicit taxonomy and comparison show why their guarantees and performance observations cannot be transferred automatically to cloud-object protection. Initial trust, authenticated interfaces, justified key processing, secure endpoints, payload encryption, and failure policy remain separate obligations. ETSI interfaces clarify delivery boundaries, while NSA and NCSC guidance highlights operational assurance concerns. Future research should connect these layers through matched, reproducible tests of both successful authenticated recovery and failure handling. The contribution is an evidence-aware synthesis and evaluation framework; no new implementation or experimental result is asserted.

Declarations

Funding: The authors received no financial support for this review.

Competing interests: No financial competing interests are declared. Omega Sarjiyus coauthored one reviewed study; this scholarly relationship is disclosed as a potential source of non-financial interpretive bias and the study is assessed using the same criteria as other evidence.

Ethics approval and consent: Not applicable. This literature review reports no new human-participant or animal research.

Data availability: No experimental dataset was generated. Appendix A provides the search expressions and source-handling approach; Appendix B records access status and consulted sources. Cited public records and accessible manuscripts constitute the evidence base.

Author contributions: Ibrahim Manga contributed to conceptualization, methodology, validation, and original drafting. Barka Mshelia Sunday contributed to conceptualization, supervision, project administration, and review and editing. Omega Sarjiyus contributed to formal analysis, investigation, and review and editing.

Use of generative AI: OpenAI ChatGPT assisted literature searching, source comparison, drafting, and editorial organization. Search and access limitations are disclosed. The authors retain responsibility for checking the final text, source interpretations, references, and submission declarations. No AI system is an author.

REFERENCES

1. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (pp. 175–179). IEEE. https://arxiv.org/abs/2003.06557
2. Buruaga, J. S., Brito, J. P., & Martin, V. (2026). Benchmarking hybrid quantum-safe cryptography over real-world infrastructures. EPJ Quantum Technology, 13, Article 75. https://doi.org/10.1140/epjqt/s40507-026-00521-y
3. Buruaga, J. S., Bugler, A., Brito, J. P., Martin, V., & Striecks, C. (2025). Versatile quantum-safe hybrid key exchange and its application to MACsec. EPJ Quantum Technology, 12, Article 84. https://doi.org/10.1140/epjqt/s40507-025-00382-x
4. Dworkin, M. (2007). Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC (NIST SP 800-38D). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-38D
5. European Telecommunications Standards Institute. (2019). Quantum key distribution (QKD); Protocol and data format of REST-based key delivery API (ETSI GS QKD 014 V1.1.1). https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf
6. European Telecommunications Standards Institute. (2020). Quantum key distribution (QKD); Application interface (ETSI GS QKD 004 V2.1.1). https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_qkd004v020101p.pdf
7. Fiorini, F., Pagano, M., Garroppo, R. G., & Osele, A. (2024). Estimating interception density in the BB84 protocol: A study with a noisy quantum simulator. Future Internet, 16(8), Article 275. https://doi.org/10.3390/fi16080275
8. Garms, L., Paraïso, T. K., Hanley, N., Khalid, A., Rafferty, C., Grant, J., Newman, J., Shields, A. J., Cid, C., & O'Neill, M. (2024). Experimental integration of quantum key distribution and post-quantum cryptography in a hybrid quantum-safe cryptosystem. Advanced Quantum Technologies, 7(4), Article 2300304. https://doi.org/10.1002/qute.202300304
9. Kim, C., Kim, S., Sohn, K., Son, Y., Kumar, M., & Kim, S. (2025). Secure and scalable file encryption for cloud systems via distributed integration of quantum and classical cryptography. Applied Sciences, 15(14), Article 7782. https://doi.org/10.3390/app15147782
10. Krawczyk, H., & Eronen, P. (2010). HMAC-based extract-and-expand key derivation function (HKDF) (RFC 5869). RFC Editor. https://doi.org/10.17487/RFC5869
11. Lee, C., Sohn, I., & Lee, W. (2022). Eavesdropping detection in BB84 quantum key distribution protocols. IEEE Transactions on Network and Service Management, 19(3), 2689–2701. https://doi.org/10.1109/TNSM.2022.3165202
12. Maned, V. R., Rath, S., Ramalingam, J., & Kuppusamy, L. (2026). Enhancing quantum key distribution via McEliece-based hybrid PQC-QKD architecture. EPJ Quantum Technology, 13, Article 33. https://doi.org/10.1140/epjqt/s40507-026-00498-8
13. Mosca, M., Stebila, D., & Ustaoglu, B. (2013). Quantum key distribution in the classical authenticated key exchange framework. In P. Gaborit (Ed.), Post-quantum cryptography (Lecture Notes in Computer Science, Vol. 7932, pp. 136–154). Springer. https://doi.org/10.1007/978-3-642-38616-9_9
14. National Cyber Security Centre. (2020, March 24). Quantum security technologies (Version 1.0). https://www.ncsc.gov.uk/paper/quantum-security-technologies
15. National Institute of Standards and Technology. (2024). Module-lattice-based digital signature standard (FIPS 204). https://doi.org/10.6028/NIST.FIPS.204

16. National Institute of Standards and Technology. (2024). Module-lattice-based key-encapsulation mechanism standard (FIPS 203). https://doi.org/10.6028/NIST.FIPS.203
17. National Security Agency. (n.d.). Quantum key distribution (QKD) and quantum cryptography (QC). https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/
18. Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shamsul Shaari, J., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., & Wallden, P. (2020). Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012–1236. https://doi.org/10.1364/AOP.361502
19. Portmann, C., & Renner, R. (2022). Security in quantum cryptography. Reviews of Modern Physics, 94(2), Article 025008. https://doi.org/10.1103/RevModPhys.94.025008
20. Prathyusha, G., Anandan, R., Venkata Krishna, P., & Saritha, V. (2026). Quantum-resilient multi-cloud encryption framework for securing big data using post-quantum lattice-based cryptography and chaotic slicing. International Academic Journal of Science and Engineering, 13(1), 30–43. https://doi.org/10.71086/IAJSE/V13I1/IAJSE1304
21. Rubio García, C., Rommel, S., Takarabt, S., Vegas Olmos, J. J., Guilley, S., Nguyen, P., & Tafur Monroy, I. (2024). Quantum-resistant Transport Layer Security. Computer Communications, 213, 345–358. https://doi.org/10.1016/j.comcom.2023.11.010
22. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S., & Bassham, L. E., III. (2010). A statistical test suite for random and pseudorandom number generators for cryptographic applications (NIST SP 800-22 Rev. 1a). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-22r1a
23. Sarjiyus, O., Adamu, U. F., & Umar, S. (2026). Enhancing cloud data security using quantum key distribution (QKD) and quantum cryptography. Proceedings of the Nigerian Society of Physical Sciences, 3, Article 266. https://doi.org/10.61298/pnspsc.2026.3.266
24. Singamaneni, K. K., Muhammad, G., & Ali, Z. (2024). A novel multi-qubit quantum key distribution ciphertext-policy attribute-based encryption model to improve cloud security for consumers. IEEE Transactions on Consumer Electronics, 70(1), 1092–1101. https://doi.org/10.1109/TCE.2023.3331306
25. Smiles, Y. W., & Sevugarajan, S. (2026). QuantumShield-IoT: A quantum-resilient hybrid framework for secure data transmission using quantum key distribution, lightweight cryptography, and blockchain technology. International Journal of Innovative Science and Research Technology, 11(7), 928–940. https://doi.org/10.38124/ijisrt/26jul281
26. Tomamichel, M., Lim, C. C. W., Gisin, N., & Renner, R. (2012). Tight finite-key analysis for quantum cryptography. Nature Communications, 3, Article 634. https://doi.org/10.1038/ncomms1631
27. Ul Ain, N., Waqar, M., Bilal, A., Kim, A., Ali, H., Ullah Tariq, U., & Shahroz Nadeem, M. (2025). A novel approach based on quantum key distribution using BB84 and E91 protocol for resilient encryption and eavesdropper detection. IEEE Access, 13, 32819–32833. https://doi.org/10.1109/ACCESS.2025.3539178
28. Wang, L.-J., Zhang, K.-Y., Wang, J.-Y., Cheng, J., Yang, Y.-H., Tang, S.-B., Yan, D., Tang, Y.-L., Liu, Z., Yu, Y., Zhang, Q., & Pan, J.-W. (2021). Experimental authentication of quantum key distribution with post-quantum cryptography. npj Quantum Information, 7, Article 67. https://doi.org/10.1038/s41534-021-00400-7
29. Wegman, M. N., & Carter, J. L. (1981). New hash functions and their use in authentication and set equality. Journal of Computer and System Sciences, 22(3), 265–279. https://doi.org/10.1016/0022-0000(81)90033-7
30. Xu, F., Ma, X., Zhang, Q., Lo, H.-K., & Pan, J.-W. (2020). Secure quantum key distribution with realistic devices. Reviews of Modern Physics, 92(2), Article 025002. https://doi.org/10.1103/RevModPhys.92.025002