Vol. 8, No. 1, February 2026

ISI Journal of Information Systems and Informatics

Published By Asosiasi Doktor Sistem Informasi Indonesia

Towards Cloud-Based Electronic Health Records in Healthcare Systems: Security, Scalability, and Migration Strategies: A Systematic Literature Review

Musawenkosi Moyo[1], Belinda Ndlovu[2]

[1,2]Department of Informatics and Analytics, National University of Science and Technology, Bulawayo, Zimbabwe

Received:
December 12, 2025
Revised:
January 15, 2026
Accepted:
January 29, 2026
Published:
March 1, 2026

Corresponding Author:
Author Name*:
Belinda Ndlovu
Email*:
belinda.ndlovu@nust.ac.zw

DOI:
10.63158/journalisi.v8i1.1431

Abstract. Cloud-based Electronic Health Records (EHRs) are being adopted rapidly worldwide, but implementation still encounters recurring obstacles in security assurance, elastic scalability, and migration readiness. Prior reviews often treat these issues separately, leaving limited practical guidance for organizations planning end-to-end deployment. This study synthesizes recent evidence on cloud EHR adoption by examining how security controls, scalability claims, and migration strategies interact in real implementation contexts. A systematic literature review following PRISMA guidelines was conducted across ACM Digital Library, PubMed, IEEE Xplore, and ScienceDirect, covering peer-reviewed studies published from 2021 to 2025. Results show that the literature is technically mature in proposing encryption, access control, auditing, and performance optimization, and frequently reports scalability advantages. In contrast, evidence on complete migration pathways—data mapping, interoperability, validation, cutover planning, and post-migration assurance—remains sparse, with many studies relying on simulations rather than longitudinal deployments. The review also identifies geographic concentration in high-income settings, limiting generalizability to resource-constrained health systems. By integrating security, scalability, and migration readiness within a socio-technical, implementation-oriented perspective, this review provides actionable directions for secure and scalable cloud EHR transitions.

Keywords: cloud-based EHR; migration readiness; healthcare cybersecurity; scalability; systematic literature review

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

1. INTRODUCTION

Electronic Health Records (EHRs) have become foundational digital infrastructures for managing longitudinal patient data, supporting clinical decision-making, continuity of care, and health-system coordination [1], [2]. While EHRs offer substantial benefits in information accessibility and service integration, their implementation remains constrained by high capital costs, security vulnerabilities, and governance challenges [1], [3]. Research consistently reports persistent weaknesses in access controls, audit mechanisms, and workforce capacity, exposing healthcare organisations to confidentiality breaches and integrity failures [2], [3], [4], [5].

Cloud computing has emerged as a dominant deployment paradigm for modern EHR systems, enabling elastic storage, scalable processing, disaster recovery, and pay-as-you-go cost structures [6], [7], [8]. However, existing reviews also highlight critical organisational and regulatory risks, including vendor dependency, opaque service-level agreements, data residency uncertainty, and misalignment with stringent health-data protection regulations [6], [7], [8], [9] . For healthcare organisations already operating under infrastructure and bandwidth constraints, these trade-offs render cloud-based EHR migration both strategically attractive and operationally complex.

A growing body of work examines how emerging architecture changes this landscape. Comprehensive reviews of IoT cloud-based e-health systems show that continuous data collection from sensors and wearable devices increases the volume, velocity, and sensitivity of information that must be secured in the cloud [10]. Systematic reviews on security and privacy technologies in health information systems further reveal that techniques such as homomorphic encryption, attribute-based access control, auditing frameworks, and differential privacy are often proposed and evaluated in isolation rather than as part of integrated cloud-EHR architectures [3], [11]. Reviews of edge-computing in smart healthcare highlight opportunities to offload latency-sensitive processing closer to the point of care, but also describe new attack surfaces, complex trust boundaries, and additional requirements for identity management and secure data synchronization between edge nodes and cloud data centers [11], [12].

To strengthen integrity and patient control in cloud-based EHRs, several systematic reviews assess the promise of blockchain and distributed-ledger technologies [13], [14]. These studies report that blockchain can provide tamper-evident logging, decentralized consent management, and fine-grained provenance tracking for EHR access, yet they also caution that throughput limits, scalability constraints, and interoperability challenges remain major barriers to real-world deployment in large hospitals and national health systems [13], [14]. More recent work proposes integrated blockchain-enabled frameworks for interoperability, data exchange, and security in healthcare, but empirical evaluations are still limited to pilots or laboratory settings, with little evidence from routine clinical use in low and middle-income countries [14].

Parallel strands of cloud-computing research address risk, migration, and organizational readiness. Systematic literature reviews on risk analysis in cloud migration and on risk assessment in cloud computing identify recurrent technical and organizational vulnerabilities, including data-loss risk, vendor lock-in, misconfigured access policies, and immature governance practices [15], [16]. A related SLR on cloud-computing security synthesizes threat taxonomies and mitigation strategies, but is largely sector-agnostic and gives limited attention to mission-critical health information systems [9]. Organizational readiness reviews in healthcare add that leadership commitment, culture, resource availability, and staff capability strongly shape whether digital transformation initiatives succeed or stall [17]. However, these studies rarely zoom in on the specific demands of migrating legacy, tightly coupled EHR infrastructures to distributed cloud platforms under strict regulatory and availability constraints.

Collectively, current systematic reviews provide rich but fragmented insight. EHR-security reviews often do not clearly distinguish between on-premise and cloud-hosted deployments [1], [3] eHealth-cloud and storage reviews treat scalability, security, and migration largely as separate design concerns [6], [7], [10] Blockchain and edge-computing reviews focus on component technologies without embedding them in realistic organizational adoption and governance pathways [11], [14] and cloud-risk and readiness reviews seldom examine the lived experience of clinicians, IT teams, and managers during EHR cloud migration projects [15], [17]. Across these streams, many proposed solutions are demonstrated in controlled testbeds or simulations, with limited empirical evidence on their performance in day-to-day clinical operations or in low-resource health systems.

Although several systematic reviews have examined cloud computing in healthcare, security mechanisms in health information systems, and risk management in cloud environments, these dimensions are typically addressed in isolation. Existing reviews often focus on technical security controls, cloud storage mechanisms, or organisational readiness, offering limited guidance for integrated, real-world EHR migration programmes. Moreover, most prior reviews do not clearly distinguish between on-premise and cloud-hosted EHR deployments, nor do they provide implementation-oriented insights into how healthcare organisations transition legacy EHR systems under regulatory, operational, and patient-safety constraints.

Despite this growing body of literature, existing systematic reviews continue to treat cloud-EHR security, scalability engineering, and migration strategy as separate technical problems. As a result, healthcare decision-makers lack an integrated evidence base to guide real-world cloud adoption that simultaneously addresses cyber-risk, performance growth, organisational readiness, and regulatory compliance. There is currently no systematic synthesis that consolidates these dimensions into a unified implementation perspective for healthcare systems. This review addresses that gap by integrating security mechanisms, scalability architectures, and migration pathways into a single socio-technical adoption framework.

This review contributes (i) an evidence-based synthesis that jointly analyses security, scalability, and migration execution in cloud-based EHR programmes, (ii) a structured mapping of where empirical evidence is strong versus under-tested (e.g., availability, migration risk, and organisational readiness), and (iii) a socio-technical migration framework that translates the review findings into implementation-oriented guidance for healthcare decision makers.

Guided by this integrated perspective, the review addresses the following research questions:

1) What security implications arise from the adoption of cloud-based EHR systems in healthcare organisations?
2) What scalability and performance benefits do cloud-based EHR systems offer compared to traditional on-premise deployments?

3) What migration strategies and organisational readiness factors support secure and scalable transition of legacy EHR systems to cloud platforms?
4) What socio-technical and organisational structures shape successful cloud-based EHR adoption?

2. METHODS

This review was structured in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) [18] guidelines, including structured search (Item 7), study selection (Item 16), risk of bias assessment (Item 18), and synthesis of results (Item 20).

2.1. Database and Search Strategy

The detailed systematic search was done on 20th November 2025 across four major databases, IEEE Xplore, ScienceDirect, PubMed, and ACM Digital Library. These databases were selected due to their strong coverage of health informatics, cybersecurity, and cloud computing research, ensuring comprehensive retrieval of both biomedical and information systems scholarship. Search strings were adapted to each database's syntax (e.g., field tags and phrase handling) while preserving the same concept blocks (cloud-based EHR; security/privacy controls; scalability/performance; migration). Filters were set to (i) peer-reviewed sources, (ii) publication years 2021–2025, and (iii) English language. The 2021–2025 timeframe was selected to capture the period in which cloud-native architectures, advanced cryptographic mechanisms, and migration-oriented studies became more prominent in healthcare systems research. A simple combination of keywords and/or their synonyms was used to formulate a search strategy, which was modified to suit each database syntax as follow.

(("cloud-based EHR" OR "cloud EHR" OR "cloud computing in healthcare") AND ("security" OR "privacy" OR "encryption" OR "data protection" OR "access control" OR "cybersecurity" OR "confidentiality") AND ("scalability" OR "performance" OR "migration"))

The initial database search retrieved 18 articles from IEEE Xplore, 3 from PubMed, 8 from ScienceDirect, and 1 from ACM. The IEEE Xplore database showed a considerable research

bias towards Cloud-based EHR systems. All records were exported to Mendeley Desktop for duplicate removal and screening.

2.2. Inclusion and Exclusion Criteria

This systematic literature review only considered full-text, open-access, English-language articles focusing on Cloud-Based EHR Systems, security, scalability, or migration. Only English-language publications were included to ensure consistency in technical interpretation and to avoid translation-related ambiguity in clinical and cybersecurity terminology, in line with common practice in healthcare systematic reviews Table 1 is Inclusion and exclusion criteria. This review aims to synthesize empirical evidence, secondary reviews were excluded from the final corpus and used only to contextualize related work and terminology.

Table 1. Inclusion and exclusion criteria

Criteria	Inclusion	Exclusion
Publication type	Peer-reviewed journal and conference papers	Grey literature, editorials, book chapters, theses
Language	English Only	Non-English publications
Time frame	2021–2025	Studies before 2021
Focus area	Studies on cloud-based EHRs addressing security, scalability, or migration of cloud-based EHRs	Studies on non-cloud EHRs Non-health or unrelated technologies
Study type	Systematic literature reviews	Non-systematic reviews, reports, or opinion papers
Accessibility	Full-text available	Abstract-only sources

2.3. Eligibility and Screening

A total of 30 papers met the Eligibility standards based on whether they were peer-reviewed and published in journals or conferences. These studies underwent title and abstract screening. Two reviewers (MM and BN) independently screened titles/abstracts and then full texts against the eligibility criteria. Disagreements were resolved through

discussion and, where needed, by consensus adjudication. A screening log was maintained to record exclusion reasons at the full-text stage to support auditability. During this phase, 10 studies were excluded because they addressed non-healthcare domains, did not examine cloud-based EHRs, or lacked relevance to the formulated research questions, leaving 20 studies for full-text evaluation

2.4. Included

After the full-text eligibility review, n=5 papers were excluded for not providing sufficient methodological rigor and empirical validation. Consequently, n=15 high-quality studies met all criteria and were included in the final synthesis. These studies form the evidence base for comparative analysis of security implications, scalability benefits, and migration strategies in cloud-based EHR systems. The flow diagram for this study using PRISMA is depicted in Figure 1.

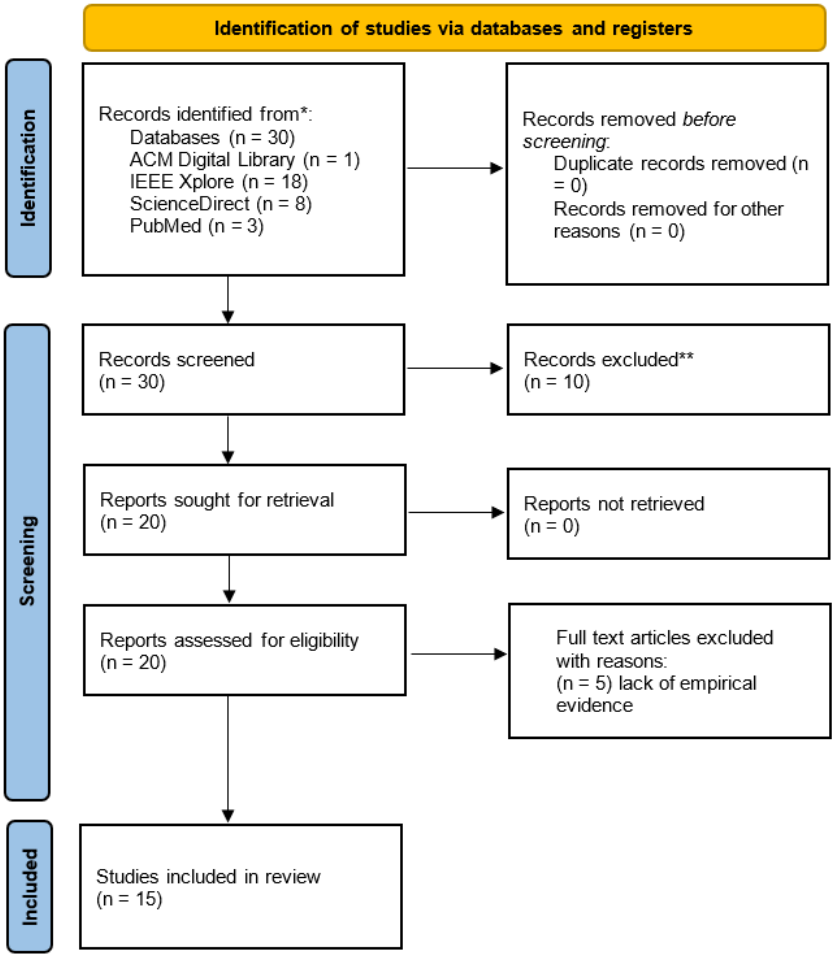

Figure 1. PRISMA Flow Diagram

2.5. Quality Assessment

Each of the 15 empirical studies was evaluated by two reviewers independently, and this was done using a simple checklist tailored to design-science, systems and case-study research. Five domains were considered:

1) Clarity of aims and relevance to cloud-based EHR security, scalability or migration.
2) Appropriateness and description of methods (example, protocol design, system implementation, case study, qualitative interviews).
3) Rigor of evaluation, including use of formal security analysis, realistic datasets or performance metrics.
4) Transparency of context and technical details (example, architecture, environment, datasets, parameters).
5) Reporting of limitations and threats to validity (example, reliance on synthetic workloads, single-site case, generalizability).

Each domain was scored on a 0–2 scale (0 = not reported/unclear, 1 = partially addressed, 2 = clearly addressed), giving a maximum quality score of 10 per study. Studies scoring 8–10 were classified as high quality, 5–7 as moderate, and 0–4 as low. Quality tiers were used analytically (not as exclusion-only): high-quality studies were weighted more strongly when drawing cross-study conclusions, while moderate/low-quality studies were used primarily to characterise gaps and methodological limitations. Each paper was given an overall judgement:

1) High quality – clear aims, appropriate and well-described methods, reasonably rigorous evaluation and at least some discussion of limitations.
2) Moderate–high quality – generally sound but with weaker reporting or more limited evaluation (example, narrow test conditions, brief limitations).
3) No paper included was assessed as low quality. The average quality score across the fifteen included empirical studies was 8.7 out of 10, indicating generally high methodological rigour, with most studies demonstrating clear aims, appropriate evaluation methods, and transparent architectural reporting. Disagreements between reviewers were resolved through discussion and consensus to ensure fairness and consistency.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Table 2. Summary of Risk of Bias Across Study Types

Aspect	Type	Description	Supporting studies
Clear problem statements and relevance	Strength	Most studies clearly stated the problem they were addressing and aligned it with cloud-based EHR security and/or scalability (e.g. secure sharing, access control, integrity, migration).	All 15 studies
Formal security analysis and/or quantitative metrics	Strength	Many studies used formal security analysis (example, GNY, BAN, ProVerif) and/or reported quantitative performance metrics such as latency, throughput and computational overhead.	[19], [20], [21], [22], [23], [24], [25]
Detailed technical descriptions	Strength	Protocols, architectures and experimental setups were usually described in enough detail to support replication or adaptation in other technical settings.	[26], [27], [21], [28], [22], [23], [29], [24], [30]
Reliance on synthetic or simulated data	Limitation/risk of bias	Most evaluations were based on synthetic datasets or lab-style simulations rather than live deployments in hospitals or health ministries.	[31], [19], [20], [27], [21], [28], [22], [23], [29], [24], [30], [25]
Limited organisational, legal and human-factor analysis	Limitation/risk of bias	Few studies have examined the organisational, legal, or human aspects of cloud-based EHR adoption; the qualitative interview study is a notable exception.	[32]
Limited external validation and LMIC evidence	Limitation/risk of bias	There was very little validation across multiple health systems or countries, and almost no empirical evidence from low- and middle-income settings.	All 15 studies (by omission)

The main strengths and potential sources of bias across the included studies were summarized in Table 2, showing good problem alignment and strong quantitative evaluation, but frequent reliance on simulated data and limited organizational and LMIC validation. Then the consolidation of these observations into the overall quality ratings is shown in table 3, indicating that most included papers were judged high quality, with a smaller portion rated moderate-high.

Table 3. Overall quality of the included empirical studies

Category	Studies	Percentage	Description	Supporting studies
High quality	12	80%	Clear aims, appropriate methods, reasonably rigorous evaluation and at least some reflection on limitations.	[19], [20], [26], [27], [21], [28], [22], [23], [33], [32], [29], [24].
Moderate–high quality	3	20%	Generally sound studies but with a more limited evaluation scope (example, simulated data only, briefer discussion of bias).	[31], [30], [25]
Low quality	0	0%	No included study was judged to be of low quality.	–

3. RESULTS AND DISCUSSION

After completing the PRISMA screening steps, we confirmed the final set of studies that met our inclusion criteria. Table 4 below summarizes the 15 included empirical papers.

Table 4. Papers that met the inclusion criteria

Author(s) / Origin	Methodology	Security Implications	Scalability Benefits	Migration Strategies	Readiness Factors	Implicit Theoretical / Paradigm Lens
[19] Saudi Arabia	Quantitative	·Authentication and key agreement · Anomity ·Attack resistance	·Lightweight crypto · Low computation/storage cost	· No explicit migration	·Technical-operational readiness	**Design Science Research (DSR)** – cryptographic authentication

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Author(s) / Origin	Methodology	Security Implications	Scalability Benefits	Migration Strategies	Readiness Factors	Implicit Theoretical / Paradigm Lens
			• Suitable at scale			protocol design + formal proof
[20] Pakistan	Quantitative	•Confidentiality • Secure cloud transmission/storage	• Faster enc/dec • Higher throughput • Suitable for high-volume mobile cloud	•Migration not addressed •Hardens existing mobile-cloud setup	-	**DSR -** security algorithm performance evaluation
[21] Thailand / Asia	Quantitative	• Access control • Efficient revocation • Prevents stale permissions	• Fog offloading • Load sharing • Lower latency at endpoints	• No organisational migration steps •Targets outsourced IoT EHR context	•Technical-operational readiness	**DSR** – access-control protocol engineering + fog architecture optimisation
[22] China	Quantitative	• Integrity assurance • Detects forged/replay proofs • Privacy-preserving auditing	• Batch auditing • Time savings at scale •Population-level verification	•Assumes EHRs already in the cloud •Post-migration assurance	•Technical-operational readiness	**DSR** – auditing scheme design and batch verification performance testing
[23] Middle East / international team	Quantitative	•Authentication and key agreement • Resists replay/impersonation/credential leakage	• Fewer rounds • Lower communication/computation cost • Scales to many users/devices	• No explicit migration guidance •Pluggable protocol	-	**DSR** – secure lightweight protocol development
[24] Multi-country team	Quantitative	•Confidentiality + integrity •Blockchain-backed logging • Non-repudiation	• Lower overhead than baselines • Efficient key/crypto operations • Mobile scalability	•Migration not covered. •Assumes mobile-cloud environment	•Technical-operational readiness	**DSR** – blockchain-enabled cryptographic system design
[25]	Quantitative	• Intrusion detection • Decoy documents	•Lightweight for edge • Practical as users/nodes grow	• No migration model	•Monitoring readiness	**DSR** – anomaly detection and decoy data security modelling

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Author(s) / Origin	Methodology	Security Implications	Scalability Benefits	Migration Strategies	Readiness Factors	Implicit Theoretical / Paradigm Lens
		• Detects insiders/masqueraders		•Add-on protection layer for edge/cloud		
[26] Multi-country /	Mixed methods	• Security-by-design via service isolation • Easier patching/monitoring	•Availability + responsiveness •Independent scaling • Better resource use	•Suggests phased refactor to microservices • No step-by-step method	•Technical-operational readiness	**DSR** + systems engineering theory (cloud microservices optimisation)
[27] Australia	Quantitative	• Integrity • Auditable access • Reduced single point of failure	•Acceptable latency/overhead •Supports many users/devices	• No explicit roadmap •Secure-sharing overlay	•Technical-operational readiness	**DSR** – blockchain-based security architecture evaluation
[28] India	Quantitative	•Confidentiality/privacy •Encryption + steganography on third-party cloud	• High throughput •Handles high transaction loads •Cloud-ready performance	• No detailed migration •Target cloud platform	-	**DSR –** encryption + steganography performance analysis
[29] USA	Quantitative	• Access control (field-level) •Context-aware authorisation • Clinical semantics alignment	• Query efficiency •Handles heterogeneous data • Scales with volume	• No detailed migration •Acts as consolidation layer	•Technical-operational readiness	**DSR** – semantic access-control modelling
[30] India	Quantitative	•Authentication (MFA) •Access control •Anomaly detection	•Acceptable delay at scale •Manageable CPU/memory use	• No explicit roadmap •Target cloud health architecture	•Technical-operational readiness •Monitoring readiness	**DSR** – multi-factor authentication and anomaly detection modelling
[31] India	Quantitative	•Confidentiality/privacy •Multi-layer encryption •Limits unauthorised access	• Cloud elasticity •Maintains performance •Supports data growth	• No explicit migration •Assumes move to cloud	-	**DSR** – multi-layer encryption framework built and tested
[32] United Kingdom (stakeholders)	Qualitative	• Trust, privacy, ownership concerns •Accountability and lock-in risks	• Perceived scalability/flexibility benefits •Constraints from	•Phased migration emphasis •Governance, skills, cost,	•Governance readiness •Leadership readiness	**Socio-technical adoption research paradigm** – interpretive

Author(s) / Origin	Methodology	Security Implications	Scalability Benefits	Migration Strategies	Readiness Factors	Implicit Theoretical / Paradigm Lens
			integration/connectivity	vendor dependence	·Workforce readiness ·Infrastructure readiness	qualitative analysis of trust & governance
[33] USA	Quantitative	· Risk reduction via safer sequencing ·Less downtime/misconfiguration risk	· Prioritises high-value dependencies · Faster service restoration	·Concrete migration method ·Dependency-aware, phased sequencing using centrality	·Risk management readiness	Operational risk decision theory / network optimisation modelling applied to migration sequencing

The synthesis of findings is organised around the four research questions, integrating architectural trends, empirical performance evidence, and organisational considerations. Rather than presenting individual studies in isolation, the analysis focuses on cross-cutting patterns, convergent design choices, and persistent implementation gaps.

3.1. Publication and Citation Trends

The timing of the studies in this review shows how quickly interest in cloud-based EHRs has grown. Before 2022, only a few papers [20], [27] appeared, mainly early blockchain-enabled sharing and security models. From 2023 onwards, there is a clear spike in publications, with a cluster of work on lightweight authentication, anomaly detection, access control and multi-layer encryption for cloud or edge-based EHR environments [19], [21]-[25], [28]-[31], [33]. This pattern mirrors broader post-COVID investment in digital health and cloud infrastructures reported in recent reviews and implementation studies, where health systems expanded telehealth, mobile health and data-sharing capabilities and turned to cloud services to keep up with demand [3], [6], [11], [15], [32].

Most empirical papers are published in open-access, technically focused outlets such as IEEE Access and other computer engineering journals [19]-[21], [23], [25], [26], [28], [30], [31]. This confirms that the conversation is currently led by the security and engineering communities rather than by clinical informatics or organizational change scholars. Consequently, the publication curve is dominated by design-science style contributions,

new protocols, cryptographic schemes and optimization techniques, while only a handful of studies take qualitative or mixed-methods perspectives that explore how cloud-EHR solutions are actually adopted and governed in practice [26], [32]. Similar imbalances between technical solutions and socio-technical evidence are noted in broader systematic reviews on healthcare cloud computing, health information security, and organizational readiness [3], [11], [12], [15], [17]. Figure 2 show distribution of included studies by publication year.

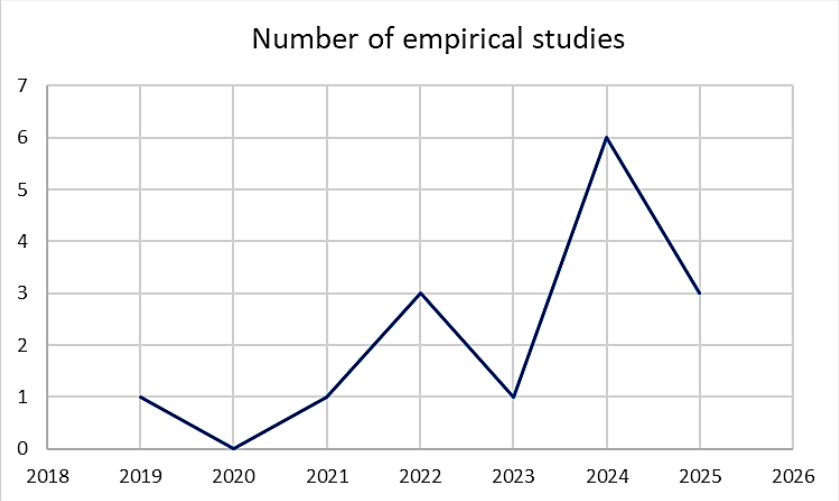

Figure 2. Distribution of included studies by publication year

Over time, the technical focus has also evolved. Early work concentrated on blockchain-based EHR sharing and secure logging [24], [27]. More recent studies move toward sophisticated authentication and access-control protocols, modular and homomorphic encryption, trust-aware access models and anomaly detection, often evaluated under simulated cloud, edge or fog computing conditions [19]-[23], [25], [28]-[31]. Despite this impressive growth in technical output, there is no comparable rise in reports of real deployments or migration projects. Only one paper in our sample describes a full data-warehouse migration for a live academic medical center, including dependency sequencing and downtime planning [33], and a single qualitative study explores stakeholder experiences of adopting cloud technologies in healthcare organizations [31]. This underlines how thin the evidence base remains for the long-term operational use of cloud-based EHR systems.

Collectively, these trends indicate a field that is expanding rapidly but remains largely isolated technically. The number of studies has risen sharply; however, conceptual integration, explicit theoretical frameworks, and real-world operational validation are still uncommon [3], [6], [11], [12], [15], [17], [19]–[26], [28]-[33]. Cloud-based EHR research is therefore best characterized as at an early engineering maturity stage, rich in proofs of concept and performance benchmarks, but comparatively lacking in implementation science. Moving forward, there is a clear need for theory-guided, longitudinal, and multidisciplinary research that examines organizational readiness, migration governance, interoperability with legacy systems, regulatory compliance, and the daily impact of cloud-EHR platforms on clinical workflows and patient trust.

3.2. Geographical Distribution

The geographical pattern tells a similar story. Most empirical studies come from Asian institutions, including Saudi Arabia, Pakistan, India and China, where investment in cybersecurity engineering and mobile-health infrastructure has been strong [19]-[21], [23]-[25], [28], [30], [31]. A smaller number of papers originate from Europe and North America [22], [26], [29], [32], [33]. None of the empirical cloud-EHR security or migration studies in our sample are set in African health systems, even though these settings often face the most acute infrastructure, funding and workforce constraints and could benefit significantly from scalable cloud solutions [15], [17]. This imbalance means that the current evidence base is likely to reflect the realities of relatively well-resourced or pilot environments, and may not generalize directly to under-resourced hospitals and ministries.

3.3. Study Characteristics/Origins

Figure 3 shows the distribution of included studies by continent. The evidence base is heavily skewed towards Asian contexts. Ten of the fifteen empirical studies were led by authors based in Asia or focused on scenarios in Asian countries such as India, Saudi Arabia, Pakistan, China and Thailand. Two studies were primarily North American, one was European, one came from Oceania, and one was explicitly multi-region. No empirical studies were identified from African settings, which reinforces the importance of context-specific work in those environments.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

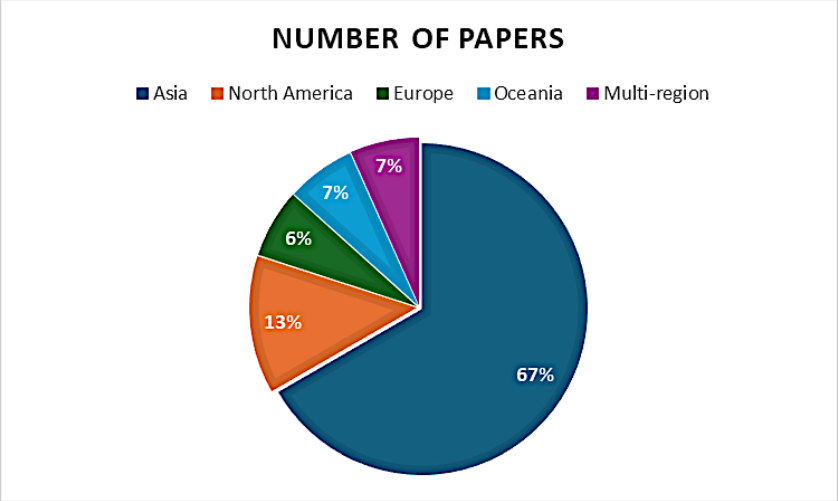

Figure 3. Distribution of included studies by continent or region.

3.4. Methodological Approaches

Figure 4 illustrates the split between quantitative, mixed, and qualitative methods across included studies. Across the fifteen included studies, the methods lean heavily towards technical "build-and-test" work. Thirteen papers used quantitative design-science or experimental approaches in which the authors propose an artefact (for example, a protocol, cryptographic scheme, auditing method or architectural framework) and then evaluate its security and performance under controlled conditions [19]-[25], [27]-[31], [33]. This pattern is consistent with the design-science tradition in information systems, where rigour is demonstrated through measurable properties such as latency, throughput, computational overhead and, in some cases, formal security proofs [34].

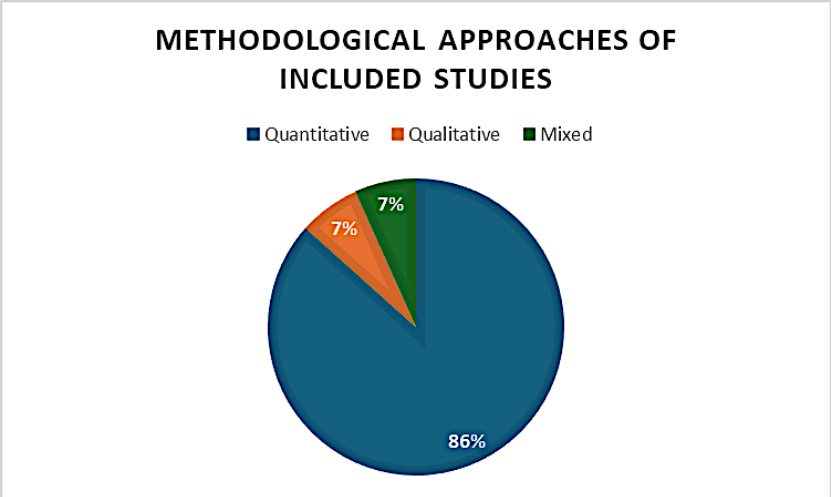

Figure 4. Methodological approaches of the included studies.

One paper combined architectural reasoning with prototype metrics and is best described as a mixed-methods design science [26]. Only a single study adopted a purely qualitative approach, using interviews and thematic analysis to explore how stakeholders experience cloud adoption, trust and privacy concerns in healthcare organizations [32].
In terms of data and evaluation settings, the technical studies predominantly relied on synthetic workloads, benchmark datasets (including intensive-care style datasets) or simulated cloud, fog and edge-computing environments rather than live hospital deployments except for [26], [32]. Where security and privacy controls were examined, the emphasis was typically on technical safeguards, encryption, authentication, access control and auditing, rather than on end-to-end organizational controls such as policy, training and governance, even though major cloud-security standards and guidance frame cloud risk as a combination of technical, administrative and operational measures [35]-[36]. Very few papers documented real-world migration work; only one study reported an operational clinical data-warehouse migration project that explicitly used dependency-based sequencing to minimize downtime and misconfiguration risk [33].

Taken together, this methodological skew towards artefact validation shows that technical feasibility studies currently dominate over organizational implementation research. While these contributions are valuable for demonstrating what is possible in terms of security and scalability, they provide limited insight into how cloud-based EHR solutions are adopted, governed, and embedded into day-to-day clinical workflows, particularly in low- and middle-income healthcare settings where constraints and risks are often greatest.

3.5. Theoretical Frameworks

Across the fifteen included empirical studies, no paper explicitly applied a formal Information Systems or behavioural theoretical framework (e.g., TOE, TAM, UTAUT, DOI, institutional or socio-technical systems theory). Methodologically, thirteen studies implicitly followed a Design Science Research paradigm, focusing on the design, development, and experimental testing of security or performance artefacts. Two studies deviated from this pattern: one adopted a qualitative socio-technical adoption perspective to investigate organisational trust and governance dynamics, and one employed operational risk optimisation modelling to support dependency-based migration sequencing. The absence of explicit theory across the technical literature

restricts explanatory understanding of cloud-EHR adoption and reinforces the need for theory-integrated implementation research. Table 5 show Implicit theoretical orientations across Included Studies

Table 5. Implicit theoretical orientations across Included Studies

Implicit Lens	Studies	Explanation
Design Science Research	13/15 technical quantitative papers	Artefacts proposed & evaluated (protocols, algorithms, frameworks)
Socio-technical adoption	[31] (UK qualitative interviews)	User trust, governance, and readiness factors
Risk management theory	[32] (migration sequencing)	Dependency risk reduction via centrality and decision optimisation
Systems theory (microservices)	[28]	Architectural decomposition for scalability & maintainability
Game/adversarial security models	[21], [22], [27]	Cryptographic and threat modelling approaches

Although none of the included studies explicitly adopted formal IS theories, 13 of the 15 papers (86.7%) implicitly align with the Design Science Research paradigm through artefact design and testing (for example, new protocols, encryption schemes, or frameworks). A small subset reflects socio-technical adoption thinking, particularly the UK qualitative interview study on cloud technology in healthcare [32], and an operational risk or migration lens in the clinical data-warehouse migration paper that uses dependency-aware sequencing to manage downtime and configuration risk [33]. However, these theoretical perspectives remain isolated and are not woven into an overarching conceptual integration across the empirical corpus.

3.6. Security Implications

Figure 5 shows that confidentiality and privacy are the most frequently reported security implications across the included studies (6 out of 15), followed by access control and authorization (4 out of 15), and integrity/auditability (3 out of 15). Other concerns, authentication/key management and intrusion/anomaly detection (2 out of 15 each), plus

availability, security-by-design architecture, and operational/migration risk (1 out of 15 each) appear much less often.

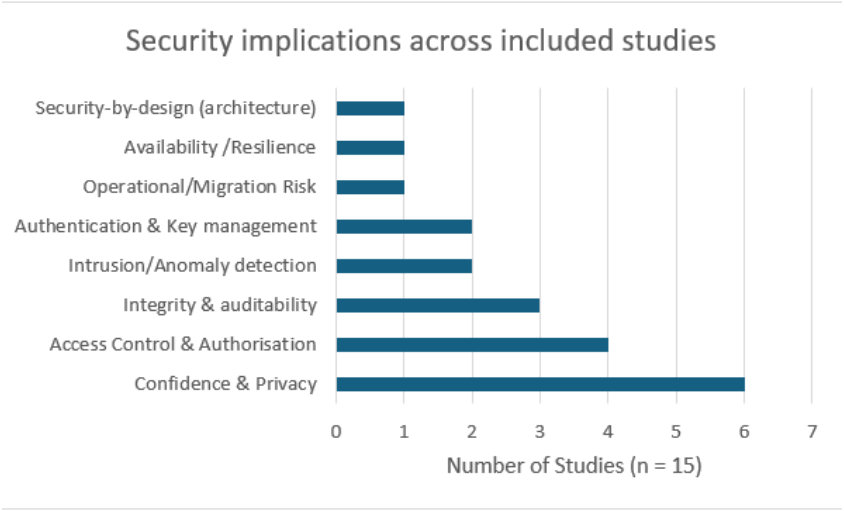

Figure 5. The number of studies rated as making a high contribution to security Implications.

3.7. Scalability Benefits

Scalability benefits were coded into five categories (performance, resource efficiency, explicit at-scale claims, offloading/load sharing, and batch/parallel processing) based on the keywords and phrases reported in the Scalability Benefits column of Table 4. Table 6 shows that performance gains and resource efficiency clearly dominate: each is reported by 6 of the 15 studies (40%), typically in the form of higher throughput, lower latency, faster response times, or reduced computational and storage overhead. Fewer papers explicitly emphasize operating "at scale" or in large-volume settings (4/15, 26.7%) [19], and only a small subset describes specific scaling mechanisms such as offloading or load sharing via fog/edge computing (2/15, 13.3%) [20], or batch-/parallel-processing strategies for population-level auditing (1/15, 6.7%). Comparative analysis across studies suggests that reported scalability gains are primarily demonstrated through short-term performance metrics rather than sustained operational growth. While many studies report improved latency or reduced overhead under simulated conditions, only a small subset explicitly addresses how these systems behave under long-term clinical workloads, organizational scaling, or evolving integration demands. This indicates that scalability in cloud-EHR research is often conceptualized as technical efficiency rather than as an organizational capability that unfolds over time.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Table 6. Shows the categories of Scalability Benefits

Scalability Category	Evidence in table 4	Supporting Studies	Percentages (of n = 15)
Performance (latency/throughput/time)	Latency reduction, throughput, increase, faster response time, time efficiency, speed, responsive	[19], [20], [21], [27], [29], [30]	40%
Resource efficiency (low overhead)	Low computational overhead, low storage overhead, lightweight, reduced resource use, memory efficiency, cost reduction	[18], [22], [23], [24], [25], [26]	40%
Explicitly at scale / large-volume	Explicit wording such as scalable, at scale, large-scale, high-volume, population-level, "works in large-scale environments."	[19], [21], [22], [28]	26.7%
Offloading/load sharing (edge/fog)	Mentions of offloading, load sharing, edge, fog, distributed processing/compute for scalability	[20], [24]	13.3%
Batch/parallel processing	Mentions of batch processing, parallel processing, "batch auditing", or similar parallelism claims	[21]	6.7%

3.8. Migration Strategies

Table 7 summarises the migration strategies identified across the fifteen included empirical studies. 86.7% of technical cloud-EHR studies provide no executable guidance on how to migrate legacy EHR systems to the cloud. Only 2 of 15 studies offer organisation-facing, real-world migration strategies.

Table 7. Migration Strategy distribution summary

Strategy Type	Studies	% of corpus	Interpretation
No migration strategy reported	10	66.7 %	Majority presume cloud state already exist
Post-migration enhancement only	3	20.0%	Focus on security/scalability of deployed systems, not migration execution.
Full organizational migration strategies	2	13.3%	Only two studies address real execution (governance planning or dependency sequencing).

Most papers (10/15; 66.7%) provided no migration guidance at all, focusing instead on post-deployment security or scalability enhancements under an assumed cloud-ready context. Three additional studies (20%) described only post-migration technical integrations without any execution pathways for legacy transition. Only two studies (13.3%) articulated practical organisational migration strategies: one emphasised phased governance-led deployment and workforce readiness, and the other presented a dependency-aware sequencing model for risk-minimised data warehouse migration. These findings highlight a major gap between technical capability research and actionable implementation science in cloud-EHR adoption. Figure 6 show studies rated as making a high contribution to research question 3.

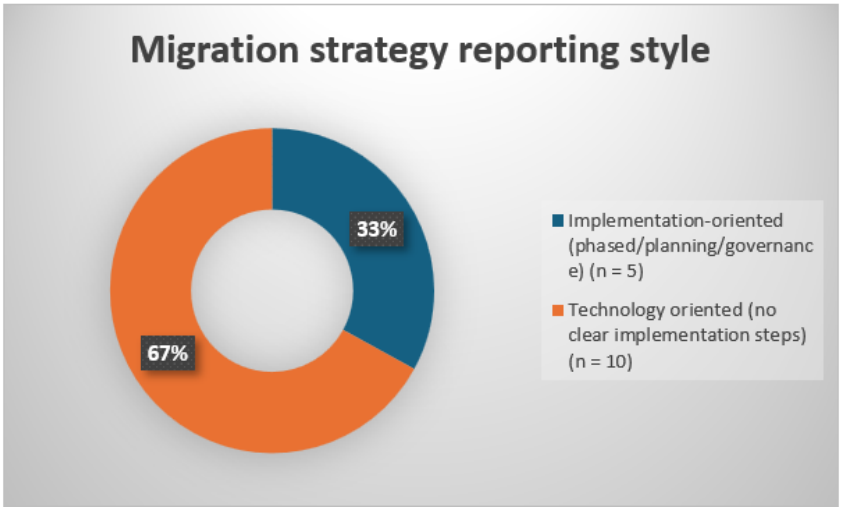

Figure 6. Studies rated as making a high contribution to research question 3

3.9. Readiness Factors

Analysis of the included empirical studies reveals a pronounced imbalance between the development of technological solutions and the investigation of organisational readiness for cloud-EHR migration. While security and scalability mechanisms are extensively engineered and validated under experimental conditions, readiness determinants that enable their safe deployment within healthcare organisations receive minimal empirical attention. Two studies directly examine organisational readiness mechanisms. They identify governance clarity, leadership coordination, staff capability development, trust formation with cloud vendors, and regulatory accountability alignment as important enablers of migration success. Risk-preparedness through dependency mapping and phased sequencing is the only systematically modelled readiness strategy documented in the literature, underscoring the importance of operational planning to reduce downtime and misconfiguration during transition. Broader readiness activities, such as identity governance, access-control policy modelling, audit infrastructure provisioning, and incident response capability, are addressed indirectly in technical artefact studies but are rarely evaluated as organisational competencies. The near absence of empirical analysis on infrastructure resilience, continuity planning, and change-management capacity further limits understanding of the feasibility of real-world implementation, particularly in low-resource health systems. Combined, the findings of the systematic review show that organisational readiness is the major bottleneck hindering migration from laboratory-proven cloud-EHR technologies and their actual, sustainable clinical adoption. This demands more studies that combine theory and field research to bring to the fore the reasons for adoption success beyond technical feasibility.

Table 8. Readiness Factors distribution summary

Readiness Factor Type	Number of Studies	% of Corpus	Interpretation
Governance & leadership	1	6.7%	Rarely studied directly
Workforce skills & training	1	6.7%	Severe evidence gap
Risk & dependency sequencing	1	6.7%	Only concretely modelled in 1 study
Cloud-native refactor readiness	1	6.7%	Largely architectural abstraction

Readiness Factor Type	Number of Studies	% of Corpus	Interpretation
Identity & access management readiness	4	26.7%	Most often discussed readiness capability
Audit & monitoring readiness	4	26.7%	Supported by security protocol literature
Infrastructure readiness (connectivity)	1	6.7%	Barely discussed

In tandem with the results, the ensuing section introduces the discussion. The findings of this review indicate that the primary challenge in cloud-based EHR adoption is not the absence of secure or scalable technical solutions, but the lack of integrated socio-technical implementation pathways. According to the reviewed literature, security, scalability, and migration are frequently treated as independent design objectives, despite their deep interdependence in real healthcare settings. This fragmentation helps explain why technically robust solutions often fail to translate into sustained organizational adoption.

In comparing data and insights across different fields, it is evident that the three aspects of security, scalability, and migration outcomes are interdependent and not independent [37]. Many proposed cryptographic and auditing solutions exhibit acceptable performance in isolation; however, their operational viability depends on architectural scaling mechanisms such as microservices deployment, fog/edge offloading, or batch and parallel processing [38]. Conversely, migration approaches that prioritize rapid data transfer without embedding identity governance, monitoring capabilities, or operational resilience introduce downstream misconfiguration and access-control risks [39], [40]. These findings indicate that secure and scalable cloud-EHR adoption requires integrated socio-technical planning linking technical controls with organizational readiness, governance, and context rather than sequential technical optimization [41], [42].

3.10. Research Question

1) RQ1: Security implications of adopting cloud-based EHR systems

Table 9 synthesizes the dominant security mechanisms reported across the literature and maps them directly to the operational risks they are intended to mitigate. This

mapping highlights that while encryption dominates current designs, broader governance, identity, monitoring, and resilience controls remain under-implemented in practice.

Table 9: Mapping of Security Controls to Operational Risks in Cloud-Based EHR Systems

Security Control	Operational Risk Addressed
Encryption	Data leakage, unauthorised disclosure
Access Control	Insider misuse, privilege escalation
Authentication	Identity compromise
Auditing	Non-repudiation, forensic readiness
Intrusion Detection	Breach detection, anomaly response
Backup and DR	Service outage, ransomware

The results show that confidentiality/privacy dominates, followed by access control and integrity/auditing. Authentication and intrusion/anomaly detection appear in only two studies each, while "security-by-design," availability, and operational/migration risk each appear in only one study. This means that the literature is very strong on "protecting data and proving security properties," but much less visible on "keeping systems safely running and governed during real adoption and migration" [43], [44].

Confidentiality and privacy: In healthcare, a privacy failure is not abstract; it damages patient trust and can halt clinical programmes [45]. That likely explains why several papers lead with encryption and privacy-preserving mechanisms [20], [24], [28], [31]. At the same time, cloud and security guidance reminds us that privacy risk is not only about encryption; it also involves data minimization, handling of personally identifiable information (PII), and clear shared-responsibility boundaries between provider and customer [36]. A few of the included technical studies show how these privacy controls are implemented alongside operational governance (e.g., account provisioning, role design, monitoring, incident response) inside real hospitals – exactly the "last mile" where privacy often fails in practice [46].

Access control and authorization: Access control appears in fewer studies than confidentiality, but it is arguably the most visible, day-to-day control clinicians experience (logins, roles, permissions, break-glass). The included studies that do focus on access

control tend to implement fine-grained, field-level or context-aware authorization [21], [29], [30], which fits the reality that EHR data is not one flat file. Broader security standards emphasize that modern cloud access control increasingly blends role-based models with attribute-based decisions and least-privilege policies, especially where context matters [39]. This has usability and workflow implications: if access control is too strict or too slow, staff workaround behaviours increase, and the "secure design" can backfire, something that is rarely measured in technical evaluations.

Integrity and auditing: Integrity and auditability matter because clinical decisions depend on data correctness and traceability over time. The evidence base includes privacy-preserving auditing schemes and tamper-evident logging approaches [22], [24], [27]. In practice, however, auditing only adds value if logs are complete, monitored and retained with clear procedures; log-management guidance treats this as an operational capability, not just a cryptographic feature [47]. A realistic gap is "operational audit readiness": few studies demonstrate how audit logs integrate with security operations center (SOC) processes, incident handling or compliance reporting in real healthcare environments.

Authentication and key management: Only two studies explicitly foreground authentication (and one combines it with access control and anomaly detection) [23], [30]. In cloud environments, identity becomes the security perimeter; weak authentication is a common root cause of breaches. Digital-identity guidance, therefore, emphasizes strong identity proofing, multi-factor authentication and lifecycle management [48], while key-management standards stress governance across key generation, storage, rotation and compromise handling [49]. The gap for cloud-based EHRs is that many papers treat authentication and keys as just a module, but real organizations need identity governance at scale (joiners/movers/leavers, emergency access, vendor accounts), especially during migration.

Intrusion/anomaly detection: Only two studies include intrusion detection or anomaly detection [25], [30], even though cloud environments are noisy and constantly changing. Intrusion-detection guidance stresses tuning, contextual awareness and response integration alerts without response plans quickly turn into "alarm fatigue" [35], [50]. A clear research gap is the evaluation of detection approaches in realistic hospital-like

operations (shift patterns, emergencies, mixed device fleets), rather than in benchmarked prototypes.

Security-by-design and isolation: One study links service level isolation in a cloud native architecture to improved security posture and maintainability, arguing that independently deployable services make patching and monitoring easier [26]. Broader cloud-computing and architecture literature similarly treats isolation boundaries, automated build/scan pipelines and frequent, small updates as first-class security controls in modern cloud environments [51], [52]. The problem is that we have almost no empirical evidence showing how cloud-native security-by-design changes outcomes in real EHR programmes (for example, deployment frequency, patch latency, or incident rates).

Availability and resilience: Only one study explicitly codes availability/responsiveness as a key implication [26]. Yet for clinicians, an unavailable EHR is not just "downtime"; it is delayed care and potential harm. Contingency planning guidance emphasizes resilience planning, backups, restoration testing and continuity procedures as critical safeguards [53]. The problem is that availability is under-measured in this 15-paper empirical set, and "acceptable latency" in a lab is not the same as resilient service under outages, degraded connectivity or cyber incidents.

Operational/migration risk: Only one paper addresses migration risk reduction in a clinical data-warehouse move, using dependency-aware sequencing to reduce downtime and misconfiguration risk [33]. Cloud-security reviews and guidance treat misconfiguration and shared-responsibility misunderstandings as persistent risks in cloud deployments[8], [9], [54], and healthcare implementation work highlights the importance of administrative safeguards and continuous risk management, not only technical controls [3], [17]. This imbalance – many security mechanisms, very few real migration-risk studies strongly support the claimed gap of this review: the field needs more empirical, organization-facing evidence on secure migration execution, not just secure end states.

2) RQ2: Scalability and performance benefits of cloud-based EHRs

The results code scalability into five categories and show that performance and resource efficiency dominate. This pattern is not surprising: many papers "prove" scalability by

showing faster encryption, acceptable overhead or higher throughput, rather than by demonstrating how systems cope with real growth in users, data and integrations over time [55].

Performance gains: Studies below define scalability through reduced latency or increased throughput under load [20],-[22], [28], [30], [31]. This fits the classic cloud promise of rapid elasticity and pooled resources, described in broader cloud and eHealth reviews [6], [7], as well as in foundational cloud-computing work on scaling out rather than scaling up [52]. However, in the empirical corpus, "performance" is almost always benchmarked in controlled environments. Very few studies test under realistic constraints such as fluctuating bandwidth, peak-hour clinical activity or multiple upstream/downstream system dependencies, even though these are precisely the conditions highlighted in cloud-migration case studies and decision-support work [40].

Resource efficiency: Studies below report lower computational or storage cost, fewer protocol rounds, or manageable CPU/memory footprints [19], [23]-[27]. In practice, this kind of efficiency matters because it reduces per-transaction cost and makes growth more affordable, particularly in resource-constrained health systems. Yet efficiency is not neutral: stronger cryptography, deeper logging or more complex access checks can increase overhead, and the SLRs on cloud storage and security note that real-world deployments need to balance these trade-offs explicitly rather than optimize one metric in isolation [7], [8]. The current corpus offers promising technical trade-offs but still provides limited operational evidence on how cloud-EHR teams tune cost and performance in production.

Explicit "at-scale" claims: A smaller subset of papers explicitly claims that their approach works for many users/devices or high-volume environments [20], [22], [23], [29]. Cloud-computing and migration guidance, however, it is clear that "scales" is not a simple yes/no label: it depends on architectural choices such as stateless service design, partitioning and caching, and on how services are operated day to day (autoscaling policies, monitoring, capacity planning, incident response) [6], [52], [40]. In our set, most evidence of "at scale" remains indirect (stress tests and simulations) rather than longitudinal usage and growth trajectories in real hospitals.

Offloading and load sharing: These are the most concrete scaling mechanisms in our results [21], [25]. These designs are closer to how large systems actually remain responsive as load increases: distributing work, pushing some computation to edge/fog nodes and parallelizing verification to avoid single bottlenecks. Related cloud-health and storage reviews point to similar patterns, where offloading and distribution are key to making security and analytics feasible on constrained devices [7], [8]. Yet only a small subset of empirical papers in this review focus on these mechanisms, suggesting a need for more end-to-end research on how EHR services remain responsive as security controls (audit, access checks, encryption) remain fully enabled.

While most studies conceptualise scalability primarily as technical performance (latency, throughput, and resource efficiency), organisational scalability refers to a healthcare institution's capacity to support sustained growth in users, data volume, and system integrations over time. Technical scalability enables elastic resource provisioning, whereas organisational scalability requires governance maturity, workforce capability, vendor coordination, and financial sustainability. The literature remains heavily weighted toward short-term performance benchmarks, with limited empirical evidence on long-term operational scalability in live clinical environments.

Across the corpus, "scalability" is operationalized primarily as short-horizon efficiency (latency/throughput/overhead), whereas evidence for longitudinal scalability under real clinical growth (users, integrations, peak-hour load, degraded connectivity) remains sparse; therefore, current claims should be interpreted as proof-of-concept scalability rather than organizational-scale readiness.

3) RQ3: Migration strategies (and readiness) for transitioning legacy EHRs to the cloud

A striking finding of this review is the rarity of empirical real-world cloud-EHR migration case studies. Only two of the fifteen included studies report real-world migration execution, underscoring a major implementation gap between laboratory-validated architectures and operational healthcare environments. The results show that most included studies are technology-oriented and provide no explicit implementation roadmap: the majority focus on hardening security or improving performance once data is assumed to be in the cloud [19]-[31], while only a small minority (around five of fifteen)

explicitly discuss phased migration, dependency sequencing, or governance and skills [21], [25], [29], [32], [33]. This mirrors broader cloud-migration research, where work on architectures and security mechanisms often outpaces detailed guidance on how organizations plan, govern and execute migration programs at scale [16], [40]. In healthcare, this gap is more serious because clinical operations, patient safety and regulatory compliance sharply raise the cost of missteps. Within this corpus, the implementation-oriented strategies we do see follow a consistent pattern: the qualitative stakeholder study surfaces real-world concerns around trust, privacy perceptions, governance, skills, integration constraints and vendor dependence [32], while the data-warehouse migration paper adds a concrete risk-reduction tactic, sequencing components by dependency to minimize downtime and configuration errors [33]. These studies read like "glimpses" of migration reality, but they are too few to establish what works reliably across diverse hospitals and ministries, especially in low- and middle-income settings where infrastructure and human-resource constraints are acute [15], [56]. A key message from both the empirical and broader literature is that security and scalability must be designed into the migration pathway, not bolted on afterwards. Cloud-security reviews and NIST guidance consistently frame migration risk in terms of misconfiguration, unclear responsibility boundaries and weak identity/access governance [3], [8], [9], [36], [39], [48], while control frameworks emphasize that monitoring, patching, incident handling and continuity processes must be part of the target operating model, not an afterthought [47], [50], [53], [52]. In other words, a migration strategy is incomplete if it only moves data; it must also move (or rebuild) security operations and performance engineering.

Finally, the results highlight a gap in the theoretical framework. No empirical paper reports an explicit IS theory in the theoretical-framework column, even though many implicitly follow a Design Science Research logic [34]. Without theory, most studies explain how mechanisms work, but struggle to explain adoption (why organisations do or do not implement them), behaviour (workarounds, trust) and change (governance, skills, institutional incentives). This is a defensible research gap for cloud-based EHR migration: future empirical work can draw on IS theories and digital-health frameworks [17], [37] to model adoption dynamics and socio-technical context, while still measuring security and performance outcomes along the migration pathway.

The evidence base remains dominated by post-deployment technical enhancements, with very limited implementation science on execution pathways (governance sequencing, workforce readiness, dependency-aware cutovers), constraining real-world decision support for healthcare migrations.

4) RQ4: Socio-technical and organisational structures of adoption

The evidence in this review suggests that the successful adoption of secure and scalable cloud-based EHRs depends less on the sophistication of the cryptography or cloud architecture on paper, and more on whether organizations can effectively embed those technologies into real clinical work. Most of the 15 empirical studies [19]-[33] focus on demonstrating the technical feasibility of encryption, authentication, auditing, and scaling under controlled conditions. Still, socio-technical models of health IT remind us that outcomes emerge from the interaction of technology, people, workflows, and wider rules and regulations [57], [58]. Systematic reviews of EMR/EHR adoption show similar patterns: strong technical potential, but recurring problems with governance structures, usability, trust, and workflow disruption when systems are deployed in practice [59].

Organizational readiness, therefore, becomes a core mechanism rather than a side issue. Evidence from low- and middle-income settings shows that weak IT governance, limited infrastructure, and fragmented leadership frequently derail EHR initiatives even when the software itself is sound [60]. Incidentally, organizational readiness studies in the global south indicate that willing management, relatively stable connectivity, and capacity-building are necessary for both successful and sustainable EHR adoption and implementation. In the body of literature under review, there was very limited reference to these concerns. One qualitative study highlights stakeholder trust, governance, and staff capability as the major drivers of cloud adoption. However, the clinical data-warehouse migration case shows how direct dependency mapping and risk sequencing can reduce downtime and misconfiguration during transition [39].

The alignment between clinical workflows and security architecture, in socio-technical terms, helps assess and explain the success and/or failure of some implementations. Robust access control coupled with strong authentication is essential. However, if they slow down clinical processes and procedures, thereby disrupting workflows, security risks Increase and Insecure actions become common [56], [57]. Previous studies on the use of

EHRs in hospitals and clinics reveal that when users are convinced of the usefulness and efficiency of the systems, it influences their willingness to adopt and sustain the digital systems. This resonated well with technology-acceptance theories such as UTAUT. Moreso, systematic evidence from the global south shows that training, focal persons, and an effective, two-way communication system are pivotal to adapt security and performance controls to frontline realities rather than expecting users simply to "fit" the system [61]. Other environmental considerations further condition cloud-EHR adoption. Reviews of EHR implementation in developing countries and other low- to medium-income countries emphasize that a country's infrastructure shortcomings, uncoordinated digital frameworks, and dependence on outsourced systems create recurring uncertainty and risk around sustainability, data Integrity, and regulatory compliance. Cloud-computing reviews in healthcare likewise advise that security, privacy, and jurisdictional issues remain major concerns when sensitive health data is processed on third-party platforms, despite clear benefits for scalability and data analytics [58]. The absence of deployment studies from African health systems in our empirical set reinforces this concern: much of the security and scalability evidence is generated in well-resourced or laboratory contexts that may not reflect bandwidth, staffing, and policy constraints in lower-resource environments.

Collectively, these findings indicate that cloud-based EHR adoption is most likely to succeed when technical innovation is coupled with deliberate socio-technical design: clear governance and accountability, realistic migration planning, strong identity and access management, ongoing training and support, and alignment with national regulatory and infrastructure conditions [34], [39]. Conversely, technically impressive but organizationally "thin" solutions risk under-use, unsafe workarounds, or outright project failure, particularly in low- and middle-income healthcare settings where resources and resilience margins are already limited.

3.11. Theoretical Frameworks

Across the 15 included empirical studies, no paper reported an explicit theoretical framework in the extracted evidence. The absence of formal IS theory application constrains explanatory insight into adoption behaviour, trust formation, organisational readiness, and governance structures. Without theoretical grounding, the literature largely demonstrates technical feasibility but struggles to explain why otherwise secure

and scalable solutions fail to translate into sustained clinical adoption. Using sociotechnical adoption frameworks such as the TOE, institutional theory, or technology trust models can help future studies do more than just prove that a tool works. These lenses make it possible to explain why implementational technology is or is not actually taken up in real organizations, and what it takes to implement it successfully in practice.

3.12. Proposed Conceptual EHR Migration Strategy Framework

The proposed framework is inductively derived from the dominant design-science, security-engineering, and migration-governance patterns identified across the fifteen high-quality studies. Each stage consolidates recurring architectural, organizational, and regulatory requirements reported in the empirical literature and translates them into an implementation-ready roadmap for healthcare cloud transformation. Figure 7 show Proposed Integrated Cloud-EHR Migration Framework.

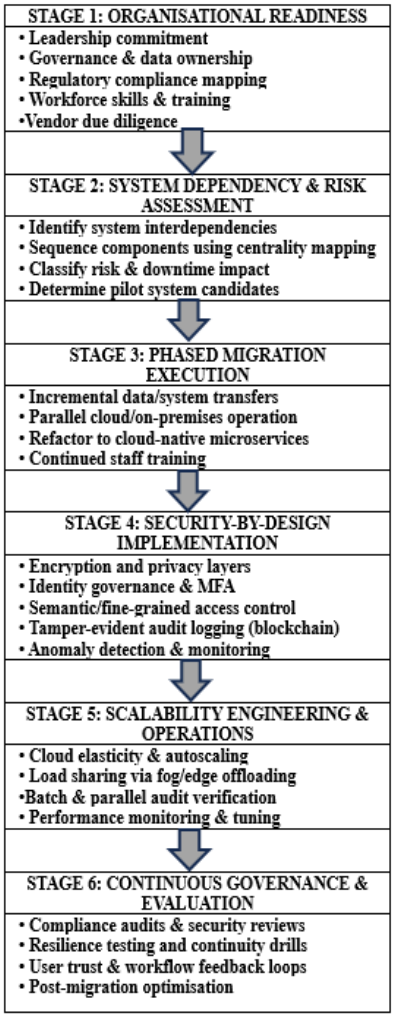

Figure 7. Proposed Integrated Cloud-EHR Migration Framework

In practice, healthcare organisations can operationalise this framework by establishing a cloud-migration steering committee, conducting readiness assessments, sequencing system dependencies, executing phased data transfer with parallel operation, and embedding security governance and performance monitoring into routine clinical operations. While the stages are presented sequentially, governance, security assurance, and scalability optimisation remain iterative throughout the lifecycle.

1) Stage 1 emphasizes organizational readiness, including governance structures, regulatory mapping, workforce skill development, leadership alignment and vendor due diligence, reflecting barriers and enablers identified by healthcare stakeholders.
2) Stage 2 introduces dependency mapping and risk-based sequencing, drawing on network-centrality techniques to prioritize low-risk, high-value components for early migration and reduce downtime, as demonstrated in the data-warehouse migration model.
3) Stage 3 focuses on migration execution, combining phased transfer and parallel operation (old and new environments running side by side) with architectural refactoring towards cloud-native, service-oriented designs to improve maintainability and fault isolation.
4) Stage 4 integrates security-by-design controls drawn from the dominant design-science literature: cryptographic protections and privacy-preserving schemes, identity and authentication mechanisms, fine-grained access-control models, anomaly or breach-detection capabilities and tamper-evident auditing approaches aligned with NIST and ABAC guidance on access control, key management and logging.
5) Stage 5 activates scalability engineering, linking cloud elasticity, fog/edge offloading and distribution with batch or parallel verification for large-scale integrity management, in line with cloud-computing guidance that treats horizontal scaling, partitioning and caching as core design principles.
6) Stage 6 stresses continuous governance and evaluation through operational security reviews, clinical usability assessments, continuity and disaster-recovery testing, compliance auditing and performance optimization, to sustain trust and service stability beyond the initial cut-over.

3.13. Implications of research findings

This review demonstrates that secure and scalable cloud-based EHR adoption is not merely a technological undertaking, but a socio-technical transformation process shaped by governance, organizational readiness, regulatory alignment, and workforce capability. From a theoretical perspective, the findings reveal a critical absence of formal adoption and institutional frameworks in existing research, limiting explanatory insight into trust formation, organizational decision-making, and sustained clinical uptake. Practically, the evidence shows that encryption and performance optimization alone are insufficient for successful deployment; healthcare organizations must integrate security-by-design, dependency-aware migration sequencing, identity governance, and continuous operational assurance into everyday clinical workflows. From a policy standpoint, the results underscore the need for EHR-specific cloud governance frameworks that address cross-border data residency, auditability, procurement safeguards, and vendor lock-in risks. Without coordinated leadership, regulatory capacity building, and implementation-oriented research agendas, cloud-EHR programmes risk remaining confined to laboratory validation rather than achieving durable health-system impact, particularly in resource-constrained healthcare environments. For clinicians, secure cloud-EHR adoption offers the potential for real-time access to longitudinal patient records, improved continuity of care across facilities, and decision-support integration, provided that security governance and workflow integration are embedded from the outset of migration programmes.

3.14. Limitations

This systematic review has several limitations that should be considered when interpreting the findings. The evidence base was restricted to peer-reviewed English-language articles indexed in the selected databases, potentially excluding relevant grey literature, government migration reports, and health system case studies documenting practical cloud deployment experiences. The final sample comprised only fifteen empirical studies, limiting geographic representation and reducing the diversity of healthcare contexts examined, particularly from African and other low-resource environments.

Most included studies relied on controlled experiments, simulations, or prototype testing rather than assessments conducted in live hospital settings. As a result, the generalisability of reported security performance and scalability metrics to real-world

clinical operations remains uncertain. Also, the near-total absence of explicit theoretical frameworks across studies constrained theory-driven interpretation of adoption behaviour, trust development, organisational change processes, and governance capacity. While systematic data extraction and synthesis procedures were applied, interpretive classification of readiness and migration factors may entail minor subjectivity. Finally, variation in reported outcomes and metrics prevented the use of statistical meta-analysis, necessitating reliance on qualitative synthesis methods.

3.15. Future Research

Future research needs to shift from mostly proving that cloud-EHR technologies can work to showing, using clear theories, how they succeed or fail when hospitals actually try to adopt them. We especially need long-term, real-world studies that follow cloud migration projects over time in different healthcare settings, particularly in low and middle-income countries. These studies should pay close attention to the practical realities, whether governance structures are ready, how staff adjust, how well the system fits clinical workflows, how reliable the infrastructure is, and whether services remain stable during and after the transition. Using well-known Information Systems theories, such as the Technology–Organization–Environment (TOE) framework, institutional theory, technology trust models, and socio-technical systems theory, can help explain adoption outcomes more deeply than simply reporting system performance.

Research should also use mixed methods to capture the full picture. That means combining hard technical evidence (such as uptime, audit-trail completeness, latency, and cost trends) with human and organizational outcomes (such as clinician trust, workflow acceptance, and leadership confidence). Comparative studies across different vendors, governance approaches, and migration sequencing strategies would help identify what works best for reducing risk, meeting compliance requirements, and building organizational resilience. On the policy side, more work is needed on national governance frameworks, cross-border data sovereignty rules, and public procurement models that enable secure, scalable EHR implementation in public health systems. Future work should validate and refine this proposed conceptual migration framework in real-world cloud-EHR projects. This can be done through empirical case studies and longitudinal evaluations across hospitals (and ideally health ministries), assessing whether the stages are practical, complete, and predictive of successful adoption, and then adjusting the

framework based on what implementation teams experience. Finally, research that directly involves clinicians, hospital administrators, IT teams, and regulators in co-designing migration approaches will make academic findings more practical and easier to apply in real healthcare settings.

4. CONCLUSION

This systematic literature review examined the security implications, scalability benefits, and migration strategies associated with cloud-based Electronic Health Records. While existing research demonstrates strong technical feasibility through encryption, access control, and scalable architectures, organisational readiness and real-world migration evidence remain limited. Most studies adopt artefact-centric validation approaches, offering little insight into governance alignment, workforce capability, workflow integration, and continuity of care during transition.

To address this translational gap, the review proposes an integrated socio-technical migration framework positioning cloud-EHR adoption as a long-term organisational transformation rather than a discrete technological upgrade. Realising the clinical and system-wide benefits of cloud-based EHRs, particularly in resource-constrained healthcare environments, will require coordinated leadership, theory-informed organisational change strategies, regulatory capacity building, and implementation-focused research agendas. These conclusions are grounded in consistent cross-study patterns observed in the empirical literature rather than speculative or normative assumptions about cloud readiness.

REFERENCES

[1] C. S. Kruse, M. Mileski, A. Ganta, S. V. Viswanathan, U. Suskandla, and Y. Chidambaram, "Impact of Electronic Health Records on Long-Term Care Facilities : Systematic Review Corresponding Author :," vol. 5, pp. 1–9, doi: 10.2196/medinform.7958.

[2] J. L. Fernández-Alemán, I. C. Señor, P. ángel O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *J. Biomed. Inform.*, vol. 46, no. 3, pp. 541–562, 2013, doi: 10.1016/j.jbi.2012.12.003.

[3] E. Mehraeen, M. Ghazisaeedi, J. Farzi, and S. Mirshekari, "Security Challenges in Healthcare Cloud Computing: A Systematic Review," *Glob. J. Health Sci.*, vol. 9, no. 3, p. 157, 2016, doi: 10.5539/gjhs.v9n3p157.

[4] R. Nowrozy, K. Ahmed, A. S. M. Kayes, H. Wang, and T. R. McIntosh, "Privacy Preservation of Electronic Health Records in the Modern Era: A Systematic Survey," *ACM Comput. Surv.*, vol. 56, no. 8, Aug. 2024, doi: 10.1145/3653297;WGROUP:STRING:ACM.

[5] R. Sibanda, B. Ndlovu, S. Dube, and K. Maguraushe, "Towards Health 4 . 0 : Blockchain-Based Electronic Health Record for Care Coordination," pp. 712–720, 2024, doi: 10.34190/ecie.19.1.2606.

[6] Y. Hu and G. Bai, "A Systematic Literature Review of Cloud Computing in Ehealth," *Heal. Informatics - An Int. J.*, vol. 3, no. 4, pp. 11–20, 2014, doi: 10.5121/hiij.2014.3402.

[7] A. Tahir *et al.*, "A Systematic Review on Cloud Storage Mechanisms Concerning e-Healthcare Systems," *Sensors (Basel).*, vol. 20, no. 18, pp. 1–32, Sep. 2020, doi: 10.3390/S20185392.

[8] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," *IEEE Access*, vol. 9, pp. 57792–57807, 2021, doi: 10.1109/ACCESS.2021.3073203.

[9] S. Drissi, M. Chergui, and Z. Khatar, "A Systematic Literature Review on Risk Assessment in Cloud Computing : Recent Research Advancements," no. April, pp. 76289–76307, 2025.

[10] C. Butpheng and K. Yeh, "SS symmetry Security and Privacy in IoT-Cloud-Based e-Health Systems — A Comprehensive Review," pp. 1–35, 2020.

[11] P. Shojaei, E. Vlahu-Gjorgievska, and Y. W. Chow, "Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review," *Computers*, vol. 13, no. 2, 2024, doi: 10.3390/computers13020041.

[12] A. Alzu'Bi, A. Alomar, S. Alkhaza'Leh, A. Abuarqoub, and M. Hammoudeh, "A Review of Privacy and Security of Edge Computing in Smart Healthcare Systems: Issues, Challenges, and Research Directions," *Tsinghua Sci. Technol.*, vol. 29, no. 4, pp. 1152–1180, 2024, doi: 10.26599/TST.2023.9010080.

[13] N. Ettaloui, S. Arezki, and T. Gadi, "Blockchain-Based Electronic Health Record: Systematic Literature Review," *Hum. Behav. Emerg. Technol.*, vol. 2024, no. 1, 2024, doi: 10.1155/hbe2/4734288.

[14] A. L. A. Fonsêca *et al.*, "Blockchain in Health Information Systems: A Systematic Review," *Int. J. Environ. Res. Public Health*, vol. 21, no. 11, pp. 1–18, 2024, doi: 10.3390/ijerph21111512.

[15] V. A. Muderere, B. Ndlovu, and K. Maguraushe, "Framework for Enhancing Interoperability, Data Exchange, and Security in Healthcare through Blockchain Technology," *Indones. J. Comput. Sci.*, vol. 14, no. 4, 2025, doi: 10.33022/ijcs.v14i4.4950.

[16] Maniah, B. Soewito, F. Lumban Gaol, and E. Abdurachman, "A systematic literature Review: Risk analysis in cloud migration," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 6, pp. 3111–3120, 2022, doi: 10.1016/j.jksuci.2021.01.008.

[17] L. Caci *et al.*, "Organizational readiness for change: A systematic review of the healthcare literature," *Implement. Res. Pract.*, vol. 6, p. 26334895251334536, Jan. 2025, doi: 10.1177/26334895251334536.

[18] D. and L. Moher Alessandro and Tetzlaff, Jennifer and Altman, Douglas G., "Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement," *PLoS Med.*, vol. 6, no. 7, p. e1000097, 2009.

[19] A. Alzahrani, "Developing a Provable Secure and Cloud-Centric Authentication Protocol for the e-Healthcare System," *IEEE Access*, vol. 12, no. November, pp. 183665–183687, 2024, doi: 10.1109/ACCESS.2024.3500216.

[20] M. Shabbir *et al.*, "Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing," *IEEE Access*, vol. 9, pp. 8820–8834, 2021, doi: 10.1109/ACCESS.2021.3049564.

[21] S. Fugkeaw, R. Prasad Gupta, and K. Worapaluk, "Secure and Fine-Grained Access Control With Optimized Revocation for Outsourced IoT EHRs With Adaptive Load-Sharing in Fog-Assisted Cloud Environment," *IEEE Access*, vol. 12, no. May, pp. 82753–82768, 2024, doi: 10.1109/ACCESS.2024.3412754.

[22] Y. Zhang, X. A. Wang, W. Jiang, M. Zhou, X. Xu, and H. Liu, "An Efficient and Secure Data Audit Scheme for Cloud-Based EHRs with Recoverable and Batch Auditing," *Comput. Mater. Contin.*, vol. 83, no. 1, pp. 1533–1553, 2025, doi: 10.32604/cmc.2025.062910.

[23] A. Delham Algarni, F. Algarni, S. Ullah Jan, and N. Innab, "LSP-eHS: A Lightweight and Secure Protocol for e-Healthcare System," *IEEE Access*, vol. 12, no. November, pp. 156849–156866, 2024, doi: 10.1109/ACCESS.2024.3477922.

[24] U. Nauman, Y. Zhang, Z. Li, and T. Zhen, "Securing Mobile Cloud-Based Electronic Health Records: A Blockchain-Powered Cryptographic Solution with Enhanced Privacy and Efficiency," *J. Intell. Med. Healthc.*, vol. 2, no. 1, pp. 15–34, 2024, doi: 10.32604/jimh.2024.048784.

[25] I. Khan, A. Ghani, S. M. Saqlain, M. U. Ashraf, A. Alzahrani, and D. H. Kim, "Secure Medical Data Against Unauthorized Access Using Decoy Technology in Distributed Edge Computing Networks," *IEEE Access*, vol. 11, no. November, pp. 144560–144573, 2023, doi: 10.1109/ACCESS.2023.3344168.

[26] J. Zaki, S. M. R. Islam, N. S. Alghamdi, M. Abdullah-Al-Wadud, and K. S. Kwak, "Introducing Cloud-Assisted Micro-Service-Based Software Development Framework for Healthcare Systems," *IEEE Access*, vol. 10, pp. 33332–33348, 2022, doi: 10.1109/ACCESS.2022.3161455.

[27] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019, doi: 10.1109/ACCESS.2019.2917555.

[28] K. Zala, H. K. Thakkar, R. Jadeja, P. Singh, K. Kotecha, and M. Shukla, "PRMS: Design and Development of Patients' E-Healthcare Records Management System for Privacy Preservation in Third Party Cloud Platforms," *IEEE Access*, vol. 10, no. August, pp. 85777–85791, 2022, doi: 10.1109/ACCESS.2022.3198094.

[29] R. Walid, K. P. Joshi, and S. G. Choi, "Leveraging semantic context to establish access controls for secure cloud-based electronic health records," *Int. J. Inf. Manag. Data Insights*, vol. 4, no. 1, p. 100211, 2024, doi: 10.1016/j.jjimei.2023.100211.

[30] S. K. B. Sangeetha, C. Selvarathi, S. K. Mathivanan, J. Cho, and S. V. Easwaramoorthy, "Secure Healthcare Access Control System (SHACS) for Anomaly Detection and Enhanced Security in Cloud-Based Healthcare Applications," *IEEE Access*, vol. 12, no. November, pp. 164543–164559, 2024, doi: 10.1109/ACCESS.2024.3492024.

[31] N. Subhalakshmi and M. V Srinath, "e-Healthsec: A Cloud-Based Privacy-Preserving Electronic Health History Framework using NLP with Multi-Layer Encryption," *Indian J. Sci. Technol.*, vol. 18, no. 6, pp. 415–429, 2025, doi: 10.17485/ijst/v18i6.51.

[32] K. Cresswell, A. Domínguez Hernández, R. Williams, and A. Sheikh, "Key Challenges and Opportunities for Cloud Technology in Health Care: Semistructured Interview Study.," *JMIR Hum. Factors*, vol. 9, no. 1, p. e31246, Jan. 2022, doi: 10.2196/31246.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[33] A. Oliver, A. A. Tariq, J. Riley, and H. Salmasian, "Optimizing the migration of a data warehouse to the cloud using network analysis," *AMIA ... Annu. Symp. proceedings. AMIA Symp.*, vol. 2024, no. Figure 1, pp. 894–899, 2024.

[34] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *J. Manag. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, 2007, doi: 10.2753/MIS0742-1222240302.

[35] J. Kizza and F. Migga Kizza, "Intrusion Detection and Prevention Systems," *Secur. Inf. Infrastruct.*, pp. 239–258, 2011, doi: 10.4018/978-1-59904-379-1.ch012.

[36] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology," doi: 10.6028/NIST.SP.800-145.

[37] T. Greenhalgh *et al.*, "Beyond Adoption : A New Framework for Theorizing and Evaluating Nonadoption , Abandonment , and Challenges to the Scale-Up , Spread , and Sustainability of Health and Care Technologies Corresponding Author :," vol. 19, doi: 10.2196/jmir.8775.

[38] M. Mrabet and M. Sliti, "Toward Secure , Trustworthy , and Sustainable Edge Computing for Smart Cities : Innovative Strategies and Future Prospects," *IEEE Access*, vol. 13, no. August, pp. 174236–174253, 2025, doi: 10.1109/ACCESS.2025.3602390.

[39] V. C. Hu *et al.*, "Guide to attribute based access control (abac) definition and considerations," *NIST Spec. Publ.*, vol. 800, p. 162, 2014.

[40] A. Khajeh-Hosseini, I. Sommerville, J. Bogaerts, and P. Teregowda, "Decision support tools for cloud migration in the enterprise," *Proc. - 2011 IEEE 4th Int. Conf. Cloud Comput. CLOUD 2011*, pp. 541–548, 2011, doi: 10.1109/CLOUD.2011.59.

[41] B. H. Banimfreg, "Healthcare Analytics A comprehensive review and conceptual framework for cloud computing adoption in bioinformatics," *Healthc. Anal.*, vol. 3, no. December 2021, p. 100190, 2023, doi: 10.1016/j.health.2023.100190.

[42] H. Sulaiman, A. Magaireh, and R. Ramli, "Adoption of Cloud-based E-Health Record through the Technology , Organization and Environment Perspective," vol. 7, pp. 609–616, 2018.

[43] D. Osamika, B. S. Adelusi, M. T. C. Kelvin-agwu, A. Y. Mustapha, A. Y. Forkuo, and N. Ikhalea, "A Systematic Review of Security , Privacy , and Compliance Challenges in Electronic Health Records : Current Practices and Future Directions," vol. 203, no. February, pp. 1–39, 2025.

[44] U. Nicole, S. Sharief, N. Grace, E. Zepka, M. Mamauag, and L. Clark, "Informatics in Medicine Unlocked Access control solutions in electronic health record systems : A systematic review," *Informatics Med. Unlocked*, vol. 49, no. July, p. 101552, 2024, doi: 10.1016/j.imu.2024.101552.

[45] V. A. Muderere, B. Ndlovu, and K. Maguraushe, "Blockchain Adoption in Healthcare : Enhancing Interoperability , Security and Data Exchange," *J. Inf. Syst. Informatics*, vol. 7, no. 3, pp. 2939–2977, 2025, doi: 10.51519/journalisi.v7i3.1267.

[46] S. Setiatin, E. A. Jakaria, and N. R. Pratami, "Analysis of Patient Data Security and Privacy in Electronic Medical Record Systems in Hospital X," vol. 3, no. 3, pp. 493–503, 2025.

[47] K. Kent and M. Souppaya, "Guide to Computer Security Log Management," *Nist Spec. Publ.*, 2006.

[48] P. A. Grassi, M. E. Garcia, and J. L. Fenton, *NIST Special Publication 800-63 - Digital Identity Guidelines*, vol. 800, no. 63. 2017.

[49] E. Barker, "NIST SP800-57 pt.1 Recommendation for Key Management: Part 1 – General," *NIST Spec. Publ. 800-57*, pp. 1–142, 2020.

[50] Karen Scarfone, Murugiah Souppaya, Sanjay Rekhi, and Alex Nelson, *NIST SP 800-61r3 - Incident Response Recommendations and Considerations for Cybersecurity Risk Management*. 2025.

[51] A. Kerman, O. Borchert, S. Rose, E. Division, and A. Tan, "Implementing a Zero Trust Architecture," *NIST Comput. Secur. Resour. Cent.*, no. July, pp. 17–17, 2020.

[52] M. Armbrust *et al.*, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010, doi: 10.1145/1721654.1721672.

[53] M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, and D. Lynes, "Contingency Planning Guide for Federal Information Systems.," *NIST Spec. Publ. 800-34 Rev. 1*, no. May, p. 150, 2010.

[54] L. Badger, R. Patt-corner, and J. Voas, "Cloud Computing Synopsis and Recommendations Recommendations of the National Institute of Standards and Technology," *Nist Spec. Publ.*, vol. 800, no. 146, p. 81, 2012.

[55] N. R. Pradhan *et al.*, "A Novel Blockchain-Based Healthcare System Design and Performance Benchmarking on a Multi-Hosted Testbed," pp. 1–20, 2022.

[56] C. Zharima, F. Grif, and J. Goudge, "qualitative study from South Africa," no. August, 2023, doi: 10.3389/fdgth.2023.1207602.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[57] A. Manuscript, "NIH Public Access," vol. 19, no. Suppl 3, pp. 1–14, 2011, doi: 10.1136/qshc.2010.042085.A.

[58] D. B. Wesley *et al.*, "A socio-technical systems approach to the use of health IT for patient reported outcomes : Patient and healthcare provider perspectives ☆," *J. Biomed. Inform.*, vol. 100, no. September, p. 100048, 2019, doi: 10.1016/j.yjbinx.2019.100048.

[59] A. Boonstra and M. Broekhuis, "Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions," 2010.

[60] A. J. Anzalone, C. R. Geary, R. Dai, S. Watanabe-Galloway, J. C. McClay, and J. R. Campbell, "Lower electronic health record adoption and interoperability in rural versus urban physician participants: a cross-sectional analysis from the CMS quality payment program," *BMC Health Serv. Res.*, vol. 25, no. 1, 2025, doi: 10.1186/s12913-024-12168-5.

[61] E. Li *et al.*, "Physician experiences of electronic health record interoperability and its practical impact on care delivery in the English NHS: a cross-sectional survey study," *BMJ Open*, vol. 15, no. 6, p. e096669, Jun. 2025, doi: 10.1136/BMJOPEN-2024-096669.