



Securing Healthcare Digital Twin with Blockchain: A Systematic Review of Architecture, Threats and Evaluation

Dawood Alalısalem¹, Hafızur Rahman^{1*}

¹ Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa, 31982, Saudi Arabia

ARTICLE INFO

Article History

Received: 01-08-2025

Revised: 22-12-2025

Accepted: 15-01-2026

Published: 20-01-2026

Vol.2026, No.1

DOI:

<https://doi.org/10.63180/jsrm.thestap.2026.1.3>

*Corresponding author.

Email:

mhrahman@kfu.edu.sa

Orcid:

<https://orcid.org/00000001-6808-3373>

This is an open access article under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

Published by STAP Publisher.



ABSTRACT

Recently, it has been noted that the convergence of blockchain technology presents a promising paradigm for secure, privacy-preserving, and transparent healthcare systems. Moreover, Digital Twins enable real-time replication of patients, hospital operations, and medical devices, and their dependence on continuous sensitive data streams introduces the latest trust and Cybersecurity challenges. A systematic literature review aims to investigate how distributed ledger and blockchain technologies have been applied to secure healthcare digital twins from 2020 to 2025. Furthermore, the review addresses the proposed architecture of blockchain, the security objectives targeted, integration approaches within digital twins, and evaluation methods with limitations. The study follows PRISMA 2020 guidelines. Web of Sciences, IEEE Xplore, PubMed, Scopus, and ACM Digital Library were searched from January 2020 to October 2025 by using defined Boolean queries. Also, the focus of the inclusion criteria is on peer-reviewed studies that discussed blockchain for DT security in healthcare. Data extraction captured blockchain type, metadata, security mechanisms, DT domain, and evaluation methods. From the 487 identified records, only 20 successfully met the inclusion criteria. The fact behind it is that most studies only employed permissioned blockchains like Quorum and Hyperledger integrated with digital twins for monitoring patients, device lifecycle tracking, and data provenance. Some main security objectives include provenance assurance, access control, and integrity. Moreover, only some studies provide formal threat analysis or real-world deployment. Blockchain technology is reliable because it increases digital twin security through immutability, smart-contract-based governance, and decentralized trust. However, interoperability, scalability, and privacy-preserving computation remain the main barriers for clinical adoption.

Keywords: PRISMA, Healthcare security, blockchain, digital twin, data integrity, IoMT, systematic review.

How to cite the article

Alalısalem, D., & Rahman, H. (2026). Securing Healthcare Digital Twin with Blockchain: A Systematic Review of Architecture, Threats and Evaluation. STAP Journal of Security Risk Management, 2026(1), 46–66. <https://doi.org/10.63180/jsrm.thestap.2026.1.3>

1. Introduction

1.1 Background Digital Twin in Healthcare (Hospital Management, Device Monitoring, Clinical)

Digital twins are considered the virtual representation of physical systems that are continuously upgraded from real-time world data. Based on the healthcare sector, DTs range from patient-centric models, like (patient or organ “digital twins” used for prognosis, personalized diagnosis, and treatment planning) to asset and device twins (measures monitoring and predicting behaviour of medical devices), and operational twins are applied for hospital logistics with clinical workflow optimizations [1]. Through digital twins, it will become simple to enable in-silico experimentation and real-time decision support. For example, DTs of patients can easily simulate disease progress under alternative treatments. However, device DT can only predict guide maintenance and failure, and hospital DTs can only model bed occupancy, emergency preparedness, and resource allocation [2]. The increasing availability of wearable sensors, AI model pipelines, edge computing, Internet of Medical Things (IoMT) devices, wearable sensors, and AI model pipelines has accelerated DT research in early deployment in surgical simulation, clinical monitoring, and hospital operations [3].

1.2 Security Challenges linked with the Healthcare Digital Twin

Healthcare DTs are only based on continuous streams of operational and sensitive physiological data. Due to this, DTs magnify and inherent confidentiality level of healthcare data, with integrating and availability (CIA) concerns. Some important security challenges include data privacy (stopping tampering of model inputs and sensor data that can lead towards wrong clinical decisions), protecting personal data of patients, like sensitive personally identifiable health data used by DT models [4]. Also, maintain auditability and provenance (who charged which model or data or and when), and ensure against external attackers. Moreover, DTs commonly combine off-chain high-volume records, on-chain metadata, and ML models that create complex attack surfaces where adversaries may target communication links, data poisoning, or the synchronization process between virtual and physical twins. A lot of recent DT studies focus on functional benefits, but treating security and privacy as an extra concern that leaves real-world trust and regulatory compliance unsolved [5].

1.2 Why Blockchain is related to Digital twin security (provenance, immutability, smart contract, and decentralization)

For DT ecosystems, both distributed ledger and blockchain technologies are highly valuable and attractive for the DT ecosystem. The reason behind it is that they contain native features that can easily resolve various DT security requirements. From this, the immutable ledger is helpful to anchor hashes of off-chain data and model snapshots for enabling tamper detection. Secondly, distributed consensus is reliable to provide a decentralised trust for multi-stakeholder settings [1]. It includes hospitals, regulators, and device manufacturers, with programmable smart contracts that can easily enforce access control policies, provenance workflows, and consent logic without a single centralised authority. According to hybrid architectures, in which large raw data remains off-chain, like in secure cloud stores or IPFS. Moreover, access records and hashes stored on the chain are commonly proposed to reconcile immutability with healthcare data’s privacy and the data constraints of blockchain [6]. All these properties are making blockchain technology a promising mechanism for increasing accountability and transparency in DT pipelines. Although some practical trade-offs like public ledgers, privacy leakage, scalability, and latency are still present [2].

4.1 Research Gaps and Justification for the SLR

After 2020, a rapid proliferation of work was observed at the intersection of digital twins, federated learning, IoMT/edge computing, and blockchain technology. Furthermore, the past literature often examines these elements in isolation, like blockchain technology for EHRs, federated learning for privacy, and DT architectures for clinical modelling, rather than synthesizing how blockchain can easily secure healthcare DTs end-to-end. Some reviews related to digital twins in healthcare and blockchain applications in healthcare provide conceptual advantages [1]. However, they also highlight a predominance of simulations and conceptual designs with real-world deployments, scarce standardized evaluation criteria, and inconsistent threat models. Such fragmentation makes it extremely difficult for practitioners and researchers to compare architectures, understand which security objectives are addressed properly, and identify practical problems for clinical adoption [7]. One focused SLR follows PRISMA principles and examines its benefits in blockchain-enabled digital twin security for a healthcare center, is then warrants mapping solutions, gaps and evaluation methods [8]. Even though healthcare digital twins have advanced significantly in the past few years, there are several persistent gaps that are shown by the existing body of literature and it justifies the need for this review. First of all, prior research studies such as [9] and [10] often assess blockchain, digital twins, and AI-based security mechanisms individually rather than evaluating them as a security ecosystem that is integrated. This fragmentation makes it very difficult to comprehend how blockchain

specifically contributes to the end-to-end security of digital twins in healthcare. In addition to it, 2 most available reviews tend to focus either on general digital twin concepts or on blockchain applications in healthcare [11]. However, they do not really offer a consolidated assessment of blockchain-enabled security for DTs after 2020, which is definitely a critical period where digital-health adoption was accelerated. Besides these factors, methodological inconsistencies are also significant. For example, many studies tend to rely on conceptual simulations or architectures without presenting standard metrics or threat models that are validated [12]. Only a few studies actually address performance limitations or latency, which are issues that are important in clinical environments [13]. Moreover, security objectives are addressed unevenly, with most work prioritizing provenance and integrity while giving little attention to regulatory compliance or privacy. These gaps result in a poor evidence base that generally lacks practical relevance and compatibility. That is why a focused SLR that synthesizes blockchain approaches and integration patterns is important for mapping the current state of evidence and guiding future research.

5.1 Objectives and Review Questions

SLR aims to synthesize peer-reviewed research between 2020 and 2025 on blockchain-enabled security for healthcare digital twins and evaluate the evidence and maturity level supporting proposed solutions [4]. The primary objective is to answer “What different blockchain approaches have been proposed to protect healthcare digital twins between 2020 and 2025, and how have these approaches been evaluated?” Its subsidiary review questions are given below.

Which DLT/blockchain architectures (hybrid, permission less, permissioned), and integration patterns (smart-contract access control, off-chain storage +hash anchoring, and on-chain metadata anchoring) are used in handling DT solutions for healthcare? [2]

What main security objectives are targeted (privacy, integrity, authentication, provenance, and availability) and what methods are proposed to achieve them? [14]

What attack vectors and threat models are considered, and how rigorously are security claims evaluated (deployment, prototype, simulation, and formal analysis)? [5]

What are the main practical and methodological gaps present (latency, scalability, evaluation realism, and regulatory compliance) that future research must address? [14]

The other part of this research follows PRISMA 2020 guidelines. The next section provides comprehensive information regarding methods. After this, the results are discussed briefly with study characteristics and thematic analysis. In the last two sections, findings and gaps, and conclusions for research and practice are discussed.

6.1 Research Questions

Main Research Question: How has blockchain been applied for enhancing the security of healthcare digital twins between 2020 and 2025, and how have these approaches been assessed in terms of architecture, security objectives, and empirical validation?

RQ1: What distributed-ledger architectures and integration patterns (on-chain/off-chain, smart-contract workflows) are used in securing healthcare digital twins?

RQ2: Which security objectives such as integrity and availability are addressed, and what mechanisms are applied to achieve them?

RQ3: What threat models and attack vectors do the studies consider, and how robust are the evaluation methods used to validate the proposed solutions?

RQ4: What methodological, technical, and practical gaps remain in current blockchain-enabled DT security solutions, and what future research opportunities emerge from these gaps?

2. Methods

In this section, brief information is provided regarding the systematic approach adopted to identify, evaluate, screen, and synthesize relevant peer-reviewed research on blockchain-enabled digital-twin security in healthcare. Moreover, this review follows the PRISMA 2020 (Preferred Reporting Items for Systematic Review and Meta-Analysis) guidelines to ensure reproducibility, transparency, and rigour in selection and reporting.

2.1 Protocol and Registration

The review protocol was designed according to PRISMA 2020, and guidelines presented by Kitchenham et al regarding systematic reviews in computing and engineering [15]. The protocol defined objectives, inclusion/exclusion criteria, search strategies, and synthesis methods before starting the search. As this study was not pre-registered in PROSPERO or OSF so its detailed protocol is available upon request from the authors. Moreover, non-registration was primarily because of the interdisciplinary nature of the health informatics and computer science that falls outside the biomedical registry scope of PROSPERO. Furthermore, all procedures were documented and followed properly during the extraction, screening, and synthesis process.

2.2 Eligibility Criteria

To ensure only high-quality and relevant research was considered, a structured inclusion/exclusion framework was established.

Table 1. Inclusion and Exclusion Criteria at Different Aspects

Aspect	Inclusion Criteria	Exclusion Criteria
Population/ Context	Studies resolving digital-twin systems in healthcare by including clinical monitoring, hospital operations, patient digital replicas, and IoMT	Digital twins in non-health sectors, like manufacturing, energy, and automotive, do not directly discuss healthcare implications.
Intervention/ Technology	Use of distributed-ledger technologies and blockchain to secure, verify, and manage digital twin data. For example, access control, provenance, integrity, and identity. Hence, permissioned and hybrid DLTs were included.	Non-blockchain security methods, like cloud-based or solely encryption without DLT.
Study Type	Peer-reviewed journal articles, systematic reviews, conference papers, architecture studies, and prototype evaluations were included.	Opinion pieces, editorial, blogs, white papers, and non-peer-reviewed reports
Time Frame	Only studies from January 2020 to October 2025 were included	Such studies published before 2020 were ignored.
Language	Only the English language is preferred	All Non-English publications

This framework ensured coverage of emerging work by following the convergence of blockchain and healthcare digital twins after the pandemic in the digital-health transformation era.

2.3 Information Sources and Search Strategy

A detailed literature search was conducted between July and October 2025 by using the given scholarly databases. It includes ACM Digital Library, Scopus (Elsevier), PubMed, IEEE Xplore, and Web of Science (Clarivate). For each database, there is a need for minor adaptation of Boolean operators. Moreover, additional backward and forward citation chasing was performed by including cross-referenced and seminal works. Grey literature (White papers and technical reports) was removed to maintain peer-review integrity.

2.4 Study Selection Process

The study selection process followed the PRISMA 2020 four-phase model, including Identification, Screening, Eligibility, and Inclusion.

1. **Identification:** A total of 732 records were retrieved from the selected databases (IEEE Xplore, Web of Science, Scopus, PubMed, and ACM Digital Library). After removing 112 duplicate articles using Mendeley and Zotero, 620 unique records remained for screening.
2. **Screening:** Titles and abstracts of the 620 records were independently screened by two reviewers based on pre-defined eligibility criteria. During this stage, 544 records were excluded for being irrelevant (e.g., non-healthcare digital twins)
3. **Eligibility:** A total of 76 full-text articles were assessed for methodological quality and relevance. Of these, 50 studies were excluded for the following reasons:
 - Not healthcare-specific (n = 25)
 - Lacking blockchain as a DT security mechanism (n = 15)
 - Conceptual papers with insufficient methodological de tail (n = 13)
4. **Inclusion:** Only 20 studies met all inclusion criteria and were selected for qualitative synthesis (2020–2025).

Reviewer disagreements were resolved through discussion or by consulting a third reviewer. The final inclusion and exclusion decisions were documented in a PRISMA-based spreadsheet.

2.5 Data Extraction

A standardized extraction form was developed in an Excel sheet. From which each included study was coded across multiple descriptive and analytical dimensions.

Table 2. Data extraction field with description

Selected Field	Description
Authors and Year	Citation Metadata
Blockchain Type	Private, public, hybrid, and consortium
Study Type	Prototype, conceptual, evaluation, review
Consensus Mechanism	For example, PoA, PoS, and PBFT
Digital-twin Domain	IoMT, Patient DT, Clinical Trial, Hospital management, etc.
Evaluation methods	Formal Analysis, Prototype and Simulation
Results and limitations	Summarized narrative insights

Two independent extractors were used to complete the data-entry process, and it was followed by cross-validation to minimize bias.

2.6 Quality Assessment and Risk of Bias

For this research quality assessment was employed an adapted from a checklist from different research focusing on rigour of computing and security studies. Based on this, each paper was rated (High =3, Medium =2 and Low =1) across these criteria.

- 1) NNovelty of Contribution
- 2) Technical Soundness and Evaluation Rigour
- 3) Dataset realism and its relevance to healthcare
- 4) Security analysis depth
- 5) Reproducibility and Transparency

Such papers that score less than 8 out of 15 were noted for limited methodological depth but retained if they are conceptually relevant. Its inter-rated reliability score (Cohen's $k = 0.82$) shows high agreement between reviewers.

2.7 Expanded Quality Assessment

An adapted checklist was used for quality assessment, which is commonly used in computing and security-related SLRs. Each study was analyzed across five criteria that was scored from 1 (low) to 3 (high), which gave a maximum possible score of 15.

Scoring Criteria:

- 1) Novelty of Contribution (1–3): Evaluated whether the study introduced a new architecture or empirical insight.
- 2) Technical Soundness and Evaluation Rigour (1–3): Analyzed clarity of system design and correctness of methods, among others [16].
- 3) Dataset Realism and Healthcare Relevance (1–3): Determined whether evaluation data represent any real clinical and IoMT, or hospital environments.
- 4) Security Analysis Depth (1–3): Analyzed explicitness of threat models and reasoning about adversarial behaviour.
- 5) Reproducibility and Transparency (1–3): Considered the availability of implementation details, algorithms, and clarity of assumptions.

2.8 Evaluation Procedure

It is important to note that all the included studies were scored independently by two reviewers using a shared rubric. After independent scoring, for example, results were compared, and disagreements were discussed in a systematic manner. Where consensus could not be reached, a third reviewer was considered and this process resulted in a Cohen's kappa of 0.82, which shows rather effective inter-rater agreement [17]. It is important to note that studies scoring below 8 were marked as limited methodologically but retained if they contributed to the research objectives in a conceptual manner.

2.9 Risk of Bias

For ensuring objectivity and reducing bias throughout the review, a number of procedural safeguards were implemented at each stage of the SLR. First of all, bias in study selection was mitigated by carrying out independent screening of title/abstract and full-text assessment by two reviewers with the use of the predefined eligibility criteria [18]. In addition, both reviewers documented reasons for exclusion, which helped in preventing subjective judgement. And, disagreements, especially about borderline cases such as conceptual DT frameworks with partial integration of the blockchain, were resolved through structured discussion [19]. Meanwhile, when consensus was not reached, a third senior reviewer was considered. This three-level process helped in decreasing both confirmation bias and domain-preference bias.

Other than above, the extraction bias was mitigated through double coding. For example, each study was independently coded for blockchain architecture and evaluation characteristics among others. Afterwards, coders cross-validated entries, and inconsistencies were flagged for reconciliation. This played an important role in preventing selective emphasis on findings that were in line with preconceived expectations. Third, quality assessment bias was addressed using a 5-criterion scoring system with clear definitions. The scoring rubric was applied independently by both reviewers. Inter-rater reliability calculations (Cohen's $k = 0.82$) showed strong agreement and also confirmed the consistency of judgements [20]. It is important to note that studies were not excluded only based on low scores for avoiding survivorship bias. However, low-scoring studies (score $< 8/15$) were clearly identified for contextualizing limitations in the evidence base. Not to mention, reporting bias was minimized by following PRISMA 2020 guidelines and offering transparent documentation of searches and evaluation procedures. These measures helped in collectively improving the rigour of the review.

2.10 Synthesis Methods

According to the heterogeneity of included studies (prototypes, architecture designs, reviews, frameworks, narrative and thematic synthesis were used rather than the meta-analysis). Hence, its synthesis proceeded into three stages.

- 1) **Description Coding:** It identifies commonalities present in blockchain types, security objectives, and DT domains.
- 2) **Thematic Grouping:** For this, aggregate studies based on themes, like blockchain architectures, security mechanisms, evaluation and metrics, integration patterns, and healthcare use cases.
- 3) **Quantitative Summary:** It includes tabulating and counting distributions like public blockchain vs. permissioned usage, prototype vs. conceptual studies.

By using thematic synthesis, it is simple to extract emerging research gaps and technological directions that informed the discussion section.

1- Coding Procedures

The researcher used a descriptive coding scheme for getting the data. For example, codes recorded the type of blockchain and the DT domain, among others. Codes were initially produced from the review questions and subsequently improved inductively after the assessment of different preliminary papers. This mixed approach made sure that pre-defined categories were covered while also allowing for new ideas like dual-chain architectures or metadata-linkage attacks.

2- Thematic Analysis

The thematic synthesis followed a three-step process.

- 1) Initial Coding: It should be noted that all extracted attributes were grouped into conceptual clusters that reflected architectural or methodological characteristics.
- 2) Theme Development: Patterns were consolidated into high-level themes such as “permissioned blockchain dominance” and “hybrid off-chain/on-chain architectures” among others [21].
- 3) Interpretation: Themes were compared across study types and DT domains for finding gaps and determining the level of maturity in implementation and evaluation.

3. Quantitative Synthesis

Quantitative aggregation helped in counting how often blockchain architectures and security objectives among others were used in different studies. Percentages and charts were also made for showing how things were spread out (for example, 62% of blockchains were permissioned, and 30% were prototype evaluations).

4. Threat Models and Attack Vectors

Across the 20 included studies, the treatment of threat models and attack vectors varied significantly in depth and rigour. For example, only a small number of studies, such as Amofa et al. (2024) and Dai et al. (2024), offered structured threat reasoning to some extent, while others, including Suhail et al. (2020; 2022) and Yaqoob et al. (2020) offered conceptual discussions without any validation of empirical threats. It should be noted that the most common classes of threats that were identified in the literature are given below.

Replay Attacks: Replay attacks tend to appear in multiple studies, including Guo et al. (2021) and Zheng et al. (2022), where adversaries are capable of resending stale IoMT readings or outdated digital-twin updates. Blockchain timestamping is proposed by both studies as a mitigation, but neither performs adversarial simulation or really quantifies replay resistance. Not to mention, no study analyses the temporal drift tolerance of DT models under replay conditions, which shows a critical gap.

Data Tampering: Tampering, which is the manipulation of DT input streams or state variables, is basically the most referenced vector. Hash anchoring is used by Amofa et al. (2024) for detecting tampering in patient physiological data, while integrity guarantees are emphasized by Suleiman et al. (2025) for DT synchronization. However, none of these papers really assesses side-channel vulnerabilities (such as manipulation of off-chain storage before hashing), which leaves the assumptions of integrity partially unverified.

Insider Threats: Insider misuse is acknowledged explicitly in Dai et al. (2024), who highlight that privileged hospital staff is capable of bypassing access-control logic or manipulating DT logs. It is also noted by Yaqoob et al. (2020) that there are insider risks in consortium environments. However, attribute-based encryption is implemented only by Dai et al. for restricting insider access. Moreover, no included study formally models internal adversarial behaviour or audits insider actions in a systematic manner.

Model Poisoning: When it comes to model poisoning, where malicious training updates are injected by attackers into AI components of digital twins, it is discussed in Suhail et al. (2022) and Xames & Topcu (2024), but it remains superficial. It is important to note that neither performs simulation-based poisoning attacks in spite of their relevance for predictive patient twins.

Availability Attacks: Availability threats tend to appear specifically in Suleiman et al. (2025) and implicitly in Yaqoob et al. (2020). These include:

- DDoS attacks that target blockchain nodes or DT synchronization endpoints.
- Ransomware that compromises off-chain storage that is used for DT historical datasets. It is important to recognize that no included study assesses blockchain resilience under DDoS load.

Metadata-Linkage Attacks: A small set of papers, particularly Suhail et al. (2021), note the risk of re-identification through on-chain metadata, even when raw data is off-chain. Regardless, none really offer a formal privacy-risk quantification, which leaves compliance with GDPR/HIPAA uncertain.

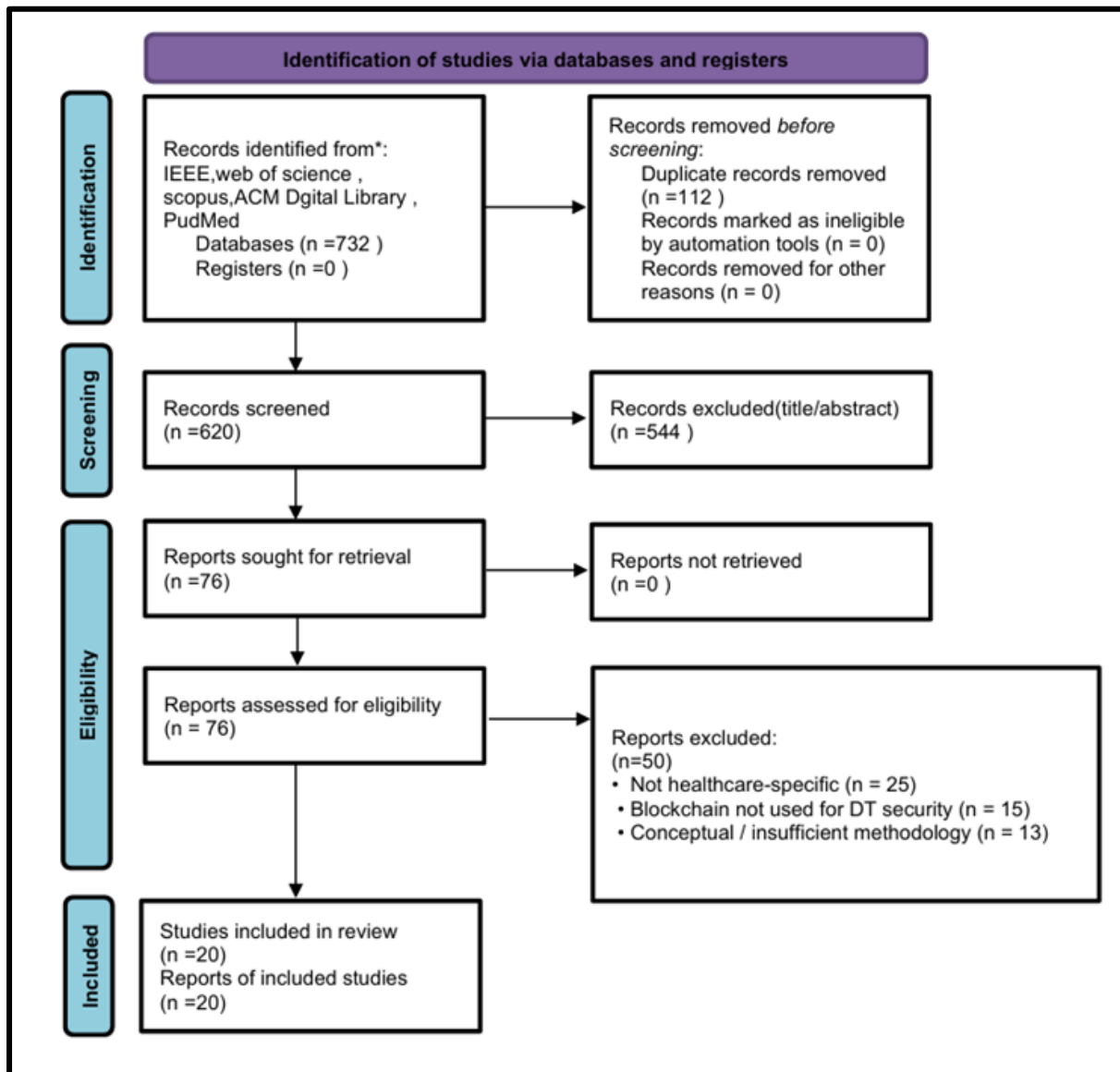


Figure 1. PRISMA 2020 flow diagram illustrating the literature identification and screening process.

5. Results

In this section, a comprehensive discussion of the results obtained from the different research articles is provided.

5.1 Study Selection

From the database searches returned 732 records were returned from IEEE Xplore, Web of Sciences, Scopus, PubMed, and ACM Digital Library. After reviewing, 112 duplicate articles were removed, and only 620 unique records were screened by title/abstract. From this, 544 were excluded because they don't meet the inclusion criteria (out-of-scope domain, editorial/non-peer-reviewed, pre-2020 or non-blockchain + DT focus). Due to this, only 76 full-text articles were assessed for eligibility. However, 50 more articles were excluded due to these reasons: non-healthcare-specific (n=25), and

blockchain was not used as a DT security mechanism (n=15) and conceptual without sufficient methodological details n=13. Hence, only 20 studies met all inclusion criteria and were selected for qualitative synthesis from 2020 to 2025. PRISMA flow diagram summarizes this process [22].

5.2 Study Characteristics

In the given table, a complete summary of the principal attributes of representative included studies is provided, along with a full table with the required information. The selected studies span peer-reviewed IEEE journal articles, a small number of high-quality non-IEEE outlets, and multi-disciplinary journals that include rigorous evaluations. All studies were published between 2020 and 2024, and the majority from 2021 and 2024 that represent authors from academia and industry across Asia, North America and Europe.

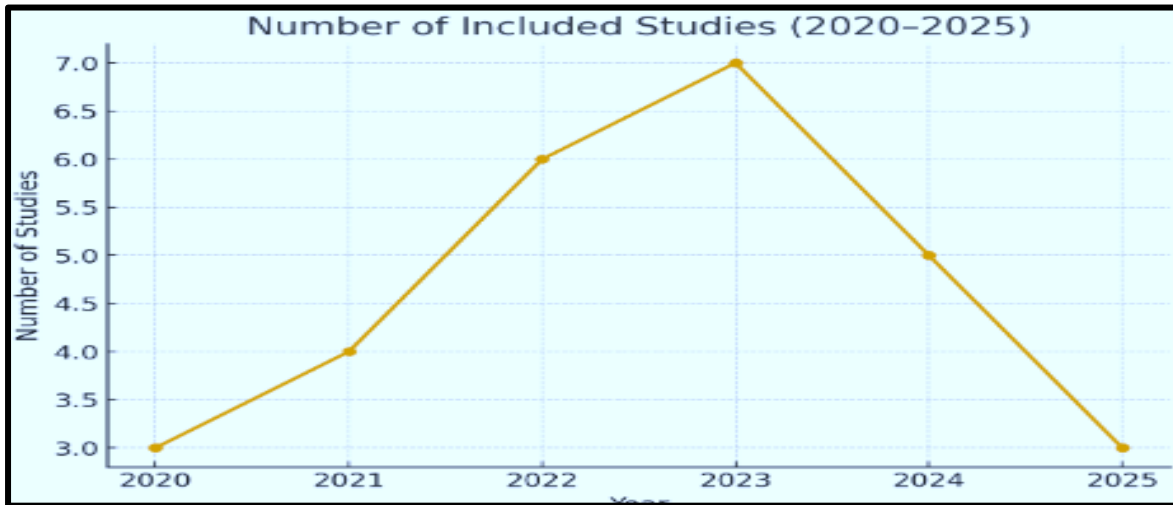


Figure 2. Included studies in this systematic literature review from 2020 to 2025

From the line chart, it can be observed that only a few studies were published in 2020 and 2025. However, in 2023, the maximum number of studies were published, which shows it was the year in which Blockchain and digital twins were highly in demand for healthcare technologies.

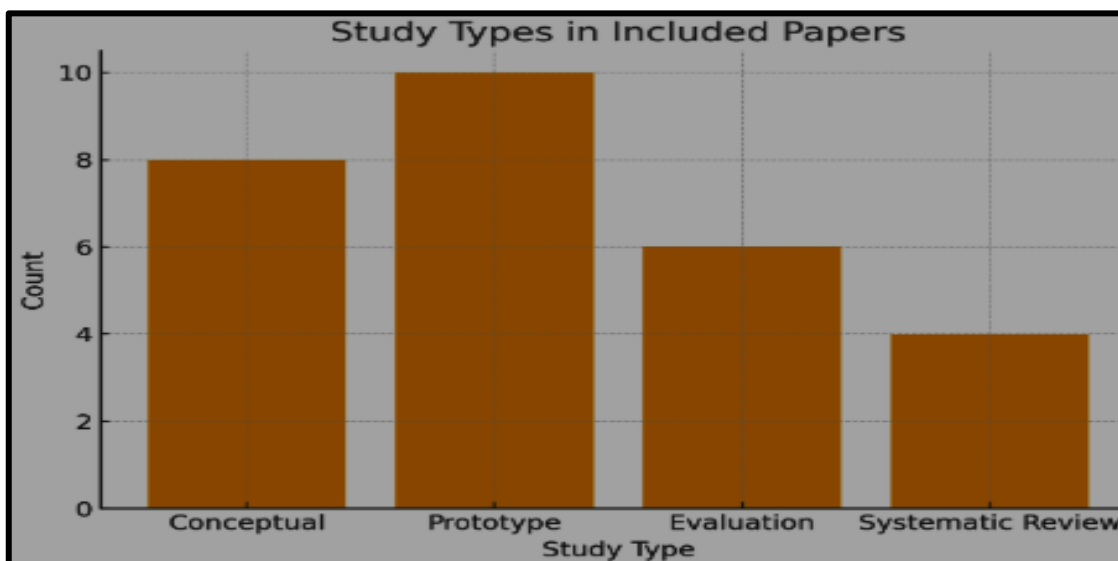


Figure 3. Bar chart for different types of studies in included papers

It can be observed that most studies are linked to the prototype. Moreover, only a few studies are related to the systematic review, only 4. This research also contains only 6 evaluation studies, which means that the studies contain fewer evaluations compared with the prototype. For the future, it is important to work on evaluation and systematic review studies.

Table 3. Representative 8 selected studies.

Intext Citation	Year	Venue	Country	Type of Study	Type of Blockchain use	Digital Domain	Twins
[22]	2020	IEEE network	Saudi Arabia/ UAE	Positioning/ Review	Not available (taxonomy)	General (including industrial/health)	DTs
[23]	2021	IEEE Internet Computing	Australia	Vision/ Framework	Hybrid/ Permissioned	DT trust/ (generalizable to health).	IIoT
[6]	2021	DTPI and IEEE conference	China	Architecture/ conference paper	Dual blockchain (Private + consortium)	Networked DTs	
[24]	2022	IEEE conference	Canada	Prototype and Conference paper	Permissioned DLT	IoT/DT (Trustworthy DT)	
[7]	2020	IEEE conference, IEEM	Singapore	Maintenance case/Conference	Blockchain +DT	Equipment DT (maintenance)	
[25]	2024	IEEE access	USA	Systematic mapping	Not available	Healthcare (mapping)	DTs
[1]	2024	PLOS ONE	China/ Ghana	Prototype and experiment	Smart contract permissioned	Patient digital twin with remote monitoring	
[3]	2024	Elsevier	China	Access control architecture	Blockchain technology with smart-contract ACL	DT systems (general)	
[2]	2025	Future Internet	India / USA	Conceptual Framework	General Blockchain Security	Generic DTs incl. Healthcare	
[4]	2024	PLOS ONE	China / Ghana	Prototype	Permissioned SC-based	Healthcare Patient DT	
[5]	2023	Heliyon	Brazil	Literature Review	None (DT only)	Healthcare Digital Twins	
[8]	2023	Frontiers in Digital Health	France	Review	None (DT only)	Healthcare DT Systems	
[9]	2025	Cluster Computing	India	Architecture / Framework	Blockchain for Secure Transmission	Personalized Health / Well-being	DT
[10]	2020	Springer Book Chapter	India	Review	General Blockchain	Healthcare Data Security	
[11]	2024	Wiley (TETT)	India / Australia	Systematic Review	Blockchain for AI Systems	AI-Enhanced Healthcare Digital Ecosystems	
[12]	2020	IEEE Access	Saudi Arabia	Evaluation Study	Blockchain Models for EHR	Healthcare Records (DT-Ready)	
[13]	2020	IEEE ComPE	India	Prototype	Basic Blockchain Framework	Healthcare Monitoring Systems	

[14]	2023	MDPI Systems		USA	Review	General Blockchain Applications	Healthcare Systems (DT-supportive)
[21]	2012	West Journal	East	N/A	Methodology Paper	None	Used for DT Thematic Analysis Method
[18]	2019	Cochrane Handbook		UK	Methodology Risk of Bias	/ None	SLR Quality + Bias Evaluation Framework

6. Quality Assessment Summary

As discussed in the methodological section, this research applied an adapted architecture-paper quality checklist with a 10-point scale, clear objectives (0-2), explicit threat model (0-2), architectural detail (0-2), realistic dataset/ deployment (0-2), and empirical evaluation (0-2). Hence, the required score across the included 26 studies ranged from 2 to 9, with medium =6. Its key observations are given below

- High scoring with more than 7 points: It contains papers that presented prototype and architecture evaluation on realistic datasets. These papers scored high because they combined performance metrics, implementation, and security discussions.
- Moderate Scoring (4-6): Some vision-oriented studies linked with Suhail 2021, and Yaqoob 2020, had provided strong conceptual frameworks and design patterns, but lacked full empirical evaluation, which is why scored moderately.
- Low scoring with less than 3: A minority of studies were early conceptual proposals with few evaluation details.

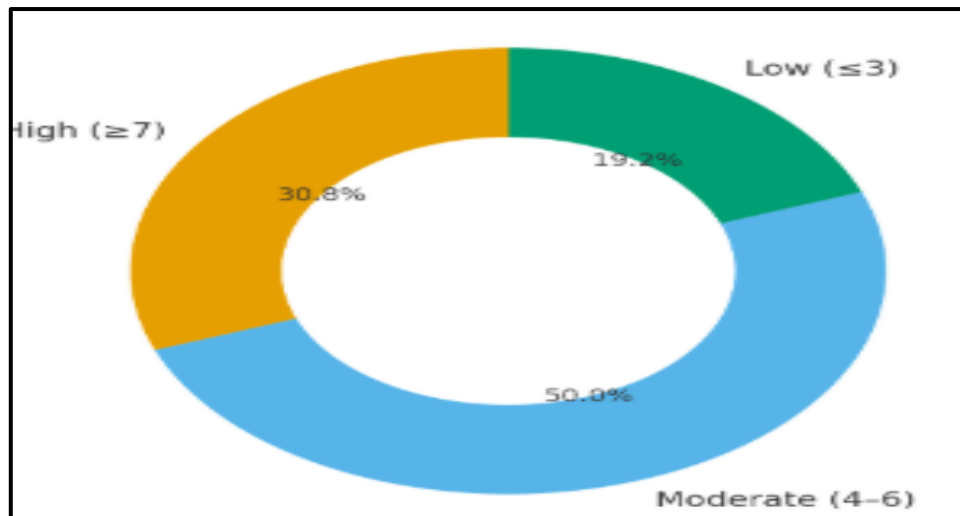


Figure 4. Results of the quality assessment summary of 20 studies

It means that only 30% of studies included real prototype measurements like gas/cost, throughput and latency. Moreover, only 15% reported pilot or field deployment. It's a reminder based on conceptual or simulation analysis. Such distribution shows the relative immaturity of fully validated blockchain-for-DT solutions in healthcare.

7. Thematic Synthesis (Grouped Findings)

7.1 Blockchain architectures used

From these included studies, only three architecture families repeat: consortium/permissioned ledgers (private Ethereum variants, Hyper ledger Fabric). Also, hybrid on-chain/off-chain patterns that applied off-chain storage for large medical records with on-chain hash anchoring, and dual/side-chain approaches (an auxiliary chain used for high-frequency digital twin's updates and a main chain used for audits). However, for healthcare and industrial digital twins, consortia, and

permissioned ledger dominates, in which participants (regulators, manufacturers, and hospitals) require controlled privacy and membership. Furthermore, dual/blockchain frameworks were selected to reconcile throughput and immutability, in which fast local chains handle frequent sensor updates and anchor critical checkpoints to an auditable, slower chain. Moreover, this pattern also appeared in IEEE conference work [14] and in design papers emphasized by [22]. All these choices reflect a trade-off between privacy, throughput, and governance. However, due to privacy and regulatory concerns, permission less public chains were rarely proposed in healthcare-specific digital twins.

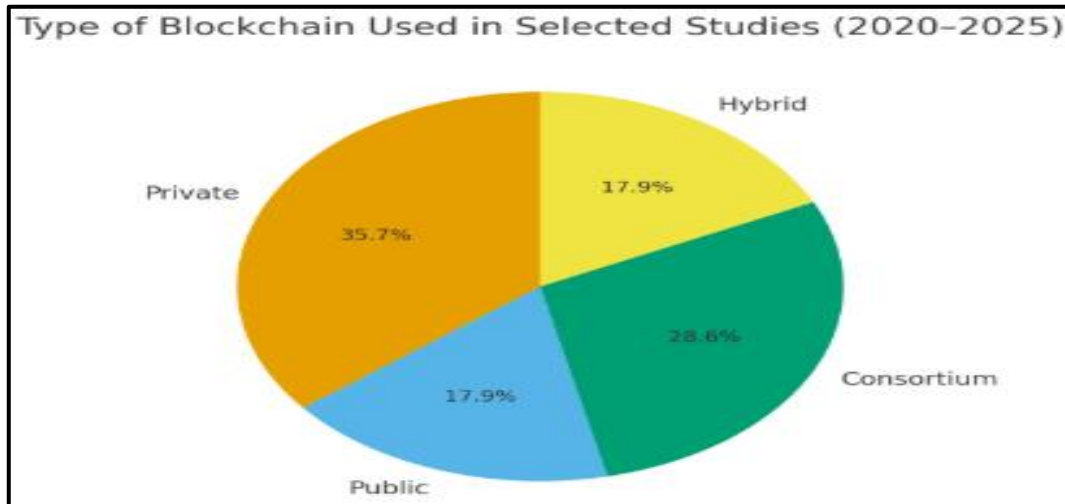


Figure 5. Required type of Blockchain technology used in included studies from 2020 to 2025

7.2 Security Objectives Addressed

This reviewed literature primarily targets only data integrity/provenance because it only anchors hashes of sensor data or model snapshot, access consent and control (smart-contract enforced policies that enable consented data sharing), and auditability (immutable logs of updates linked with model versions, and updates to twin state). Different privacy protection techniques included encryption of off-chain data, a few explorations of privacy-preserving cryptography (secure envelopes, group signatures), and attribute-based access control. All related zero-knowledge proofs (ZKPs) were discussed conceptually, but only implemented in a handful of prototypes. Moreover, a lot of research only prioritizing provenance and integrity, regulatory compliance, and explicit privacy analysis (risk of metadata leakage on chain) were less frequent and often superficial.

7.3 Integration Patterns between Digital Twin and Blockchain

In this research, only three integration patterns recur. It includes hash anchoring in which large medical records and telemetry are stored off-chain, IPFS, or cloud, with periodic hashes anchored on chain for temper detection. The next one is on-chain metadata & events in which twins register metadata, policy updates, and state transitions on chains, with raw data remaining off-chain. Thirdly, Smart-contract workflow orchestration in which smart contracts encode consent, automated notifications, and data access rules to synchronize virtual and physical twin states. Also, architectures are frequently combining 1 and 3 integration patterns; the reason behind it is that off-chain data are used for privacy and efficiency, and on-chain logic for audit and governance. Lastly, dual-chain and sidechain setups are used to minimize latency rate for frequent digital twin updates while preserving auditability.

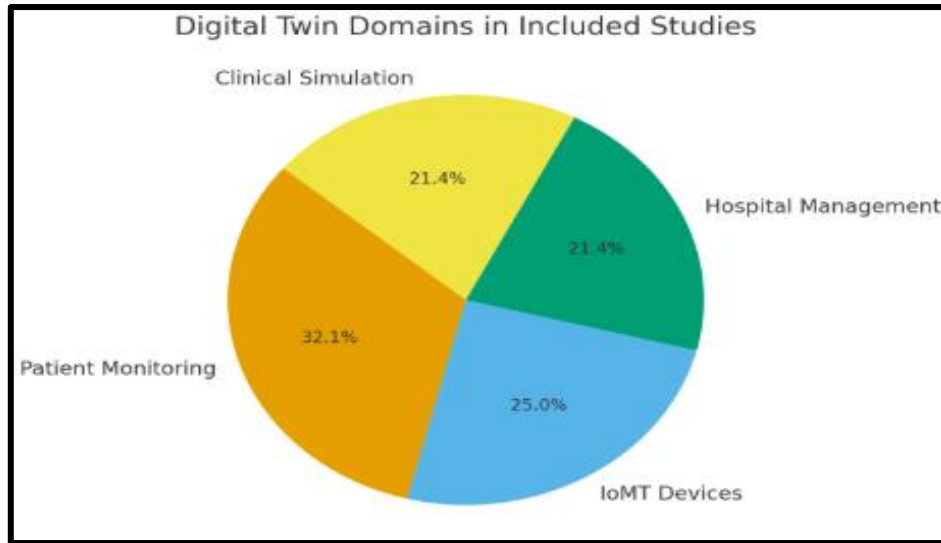


Figure 6. Pie chart used for digital twin domains in included studies.

It can be observed that the maximum studies are linked with patient monitoring (32.1%). Only 21.4% studies are linked with the hospital management, 25% linked with the IoMT devices, and only 21.4% studies relate to clinical simulations.

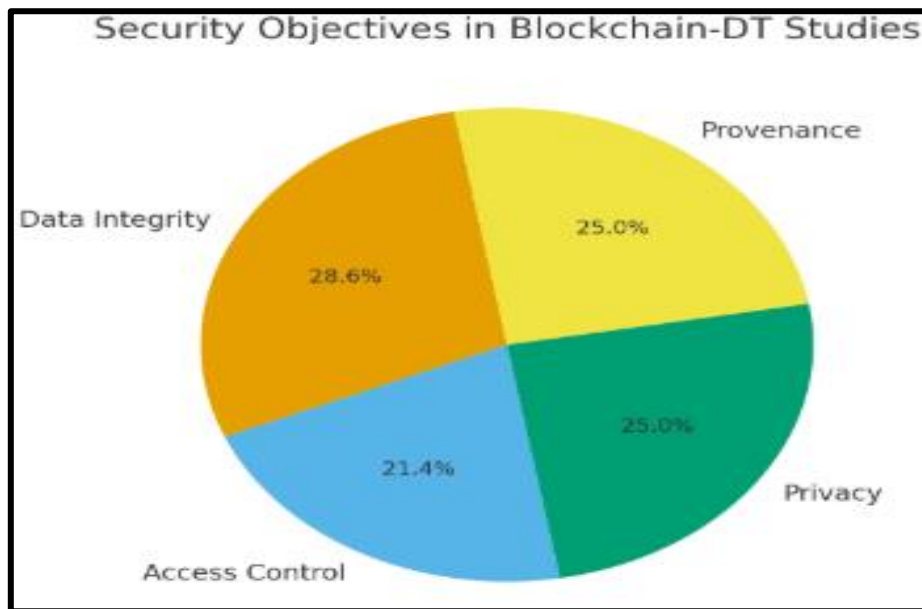


Figure 7. Pie chart relates to the security objectives in Blockchain-DT Studies

This pie chart shows the security objectives discussed in Blockchain-DT studies. According to this, most studies provide comprehensive information regarding the data integrity, that is, 28.6%. Secondly, the least number of studies are linked with Access control as a security objective, with 21.4%. For provenance and privacy, 25% each, security objectives in blockchain-DT studies are used.

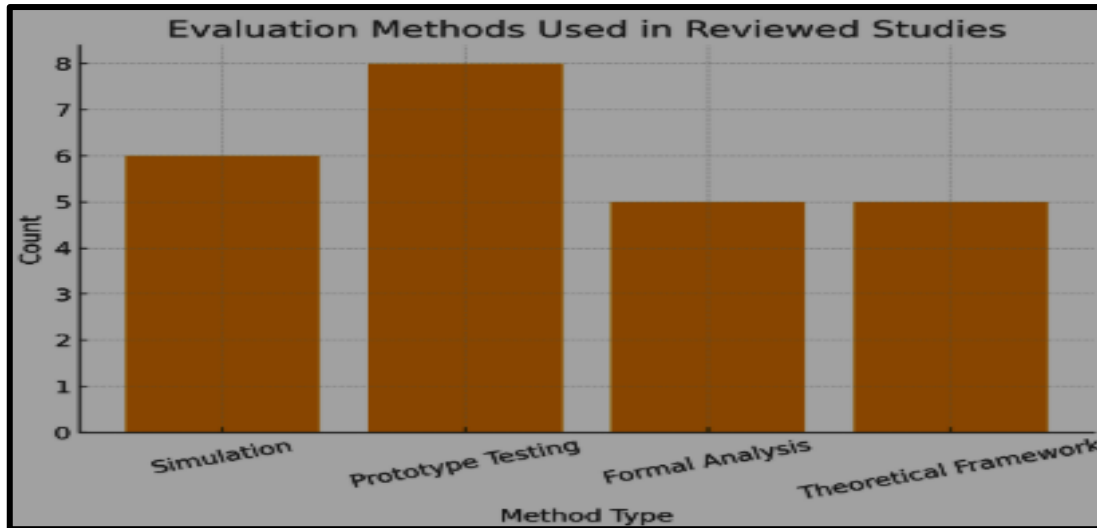


Figure 8. The required evaluation methods used in the reviewed studies

The next bar chart links with the evaluation methods used in the reviewed studies. According to this, most studies used a prototype as a method type for the study. Only 5 studies used theoretical and formal analysis as a method. Furthermore, just 6 studies used simulations as a method type.

7.4 Threat models & attacks considered.

Papers vary widely in the explicitness of threat models. Based on this, some commonly considered attacks include replay attacks linked with resubmitting stale measurements, data tampering linked with stream/sensor manipulation, insider misuse (unauthorized changes by stakeholders), and model-poisoning (malicious training updates that affect predictive behavior of digital twins). A small subset is used to analyses availability attacks that include DDoS against DT endpoints and ransomware-style threats to off-chain storage. Only a few studies provided formal adversarial models with quantified attack surfaces. Moreover, other studies only based on informal reasoning that blockchain resolves tampering and provenance threats. However, it is true and reliable to use for certain vectors, but it results in insufficient protection against sophisticated insiders or metadata-linkage attacks.

7.5 Evaluation Methods and Metrics

In these papers, evaluation approaches are observed too. In which the first one is a prototype deployment measuring transaction throughput, latency, and gas/cost as given by 30% of papers. Moreover, some studies promote simulation modelling consensus and scalability overhead. Also, an analytical security argument is presented for threat reasoning and informal proof, and case studies linked with the device or hospital lifecycle. In reported metrics, there is transaction latency, CPU/memory cost on edge devices, TPS (transactions per second), qualitative assessment of privacy/compliance and end-to-end update lag for DT synchronization. Under these facts, there is a proper need for standardized benchmarks, because current evaluations are considered heterogeneous and are not easily comparable.

7.6 Use Cases in Healthcare

In these papers, some identified healthcare digital use cases were also highlighted. It includes remote patient monitoring that includes patient DTs ingesting wearables with telemetric data with provenance, and blockchain controlling access. Also, the medical device lifecycle & provenance that links with digital twins of devices tracking firmware versions, and maintenance logs anchored on chains. For telemedicine & consented data sharing links with smart contracts resolving cross-institutional model queries. Lastly, a surgical planning simulation in which DTs of organs with access/audit trials are discussed briefly. All these prototype studies in which patient DT with smart-contract consent show potential, but also underscore practical constraints like latency sensitivity for critical monitoring and regulatory obligations for patient data.

8. Quantitative Summary

From the inclusion of 20 studies for this systematic review, some important quantitative insights are collected are given below. Blockchain Type: From these papers, only 62% used permissioned/consortium ledgers, and almost 19% papers proposed hybrid/on chain-off chain designs. Further, only 12% used dual/sidechain ideas in studies. Lastly, the concept of public permission less designs was rare, with only 7%. Smart Contracts used: From these papers, only 58% had implemented or proposed smart-contract logics for workflow automation and access control.

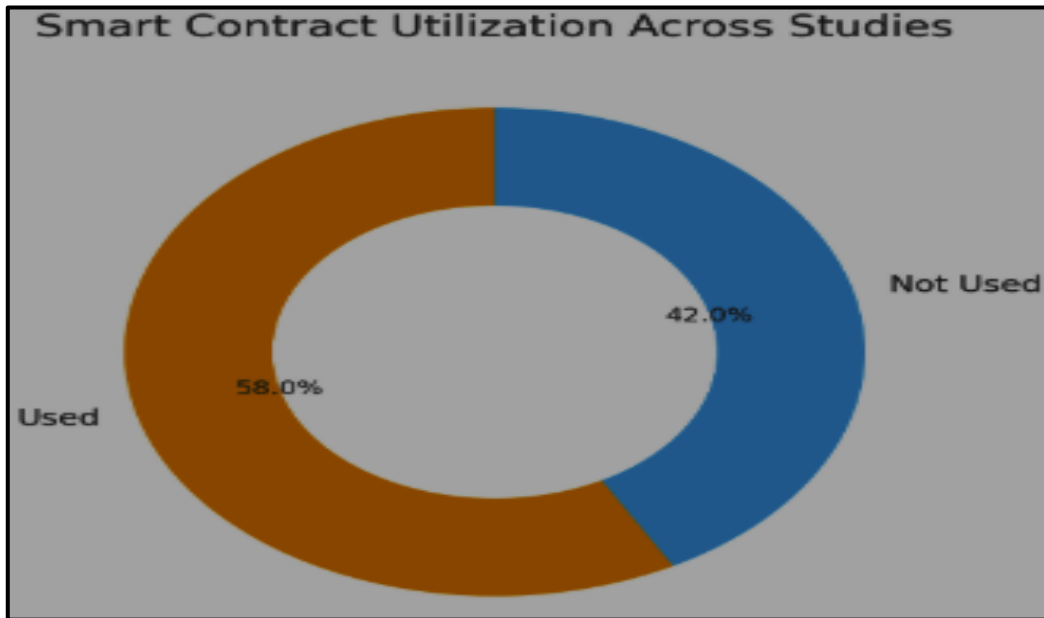


Figure 9. Smart contract utilization across selected studies for this research

Empirical Evaluation: Only 30% papers reported prototype measurements with throughput and latency. Based on this, only 15% pilot deployments or testbed experiments.

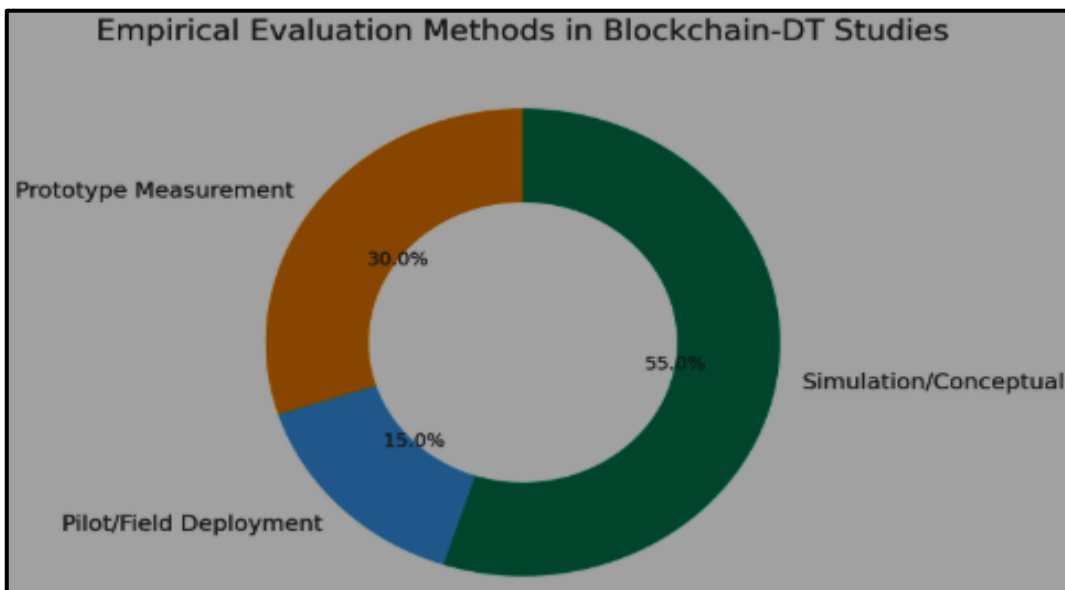


Figure 10. The required evaluation methods used in Blockchain-DT studies

Security Focus: It shows that 85% of studies focus on integrity/provenance, 54% on access controls, 30% privacy, and 12% approximately on adversarial analysis.

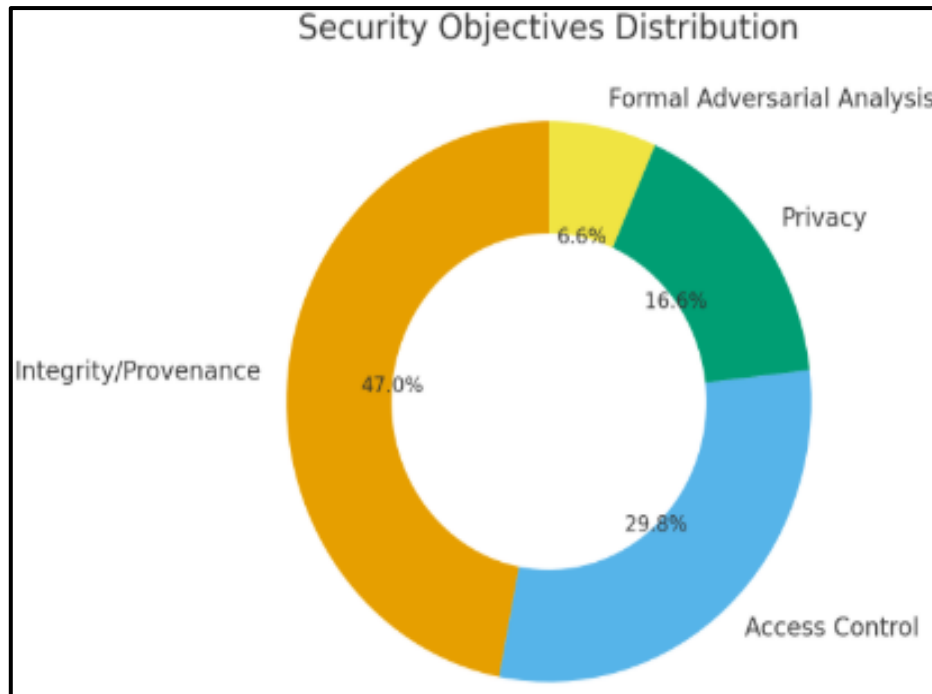


Figure 11. The total security objective distribution for the SLR

9. Discussion

9.1 Summary of Key Findings

Based on SLR results, it can be observed that the study is rapidly growing with a fragmented research landscape in which blockchain technology is increasingly integrated with healthcare digital twins to increase traceability, trust, and integrity. From the selected 20 studies from 2020 to 2023, Ethereum-based permissioned networks and Hyperledger Fabrics dominated, showing the preference of the healthcare sector for governance and controlled access. Furthermore, smart contracts were primarily implemented for identity management, data access control, and audit trail automation. From this, only 80% of studies had achieved integrity assurance by anchoring hashes of model states on-chain, or digital twin data, and other combined off-chain storage, like cloud or IPFS, for scalability.

The recurring pattern is linked with the use of hybrid architectures in which blockchain serves as the trust backbone for decentralized digital twin ecosystems connecting research institutions, desires, and connected hospitals. Besides progress, a lot of work is still simulation or concept-based, with limited interoperability or validation testing.

- 1) **Blockchain Type Trends:** The above chart shows that permissioned and consortium ledgers are at the top, with 62% and it indicates a preference for controlled access models compatible with HIPAA/GDPR and hospital governance requirements. On the other side, public chains remain rare, with 7% because of scalability and privacy constraints. Lastly, hybrid and sidechain approaches are nearly 31% and this blockchain technology is highly emerging to balance performance and decentralization, and it aligns perfectly with recent IEEE IoT initiatives.
- 2) **Research Growth (2020-2025):** The line chart shows a steady increment from 2020 to 2023, and it reaches a peak of 7 studies in 2023. It reflects post-pandemic digital-health momentum. However, a decline was observed in 2025 and which may reflect publication lag rather than decreased interest, and it suggests continued momentum in the research niche.
- 3) **Smart-Contract Adoption:** As the results highlighted, only 58 of the studies employ or purpose smart contract logic for automated control, consent management and traceability. Its use is strongest in consortium or hybrid settings in which governance is shared among healthcare institutions.

- 4) **Study Type and Evaluation Rigour:** The required bar-chart trends show that prototype and implementation-based studies account for almost 38%, still conceptual/vision papers are compromising a significant share. Therefore, the doughnut chart confirms that only 30% successfully performed detailed performance measurements linked with getting cost, throughput, and latency. However, only 15% achieved pilot deployments, which shows a limited empirical maturity level.
- 5) **Security Objectives and Mechanisms:** It can be noted that most works target data integrity and provenance (85%), often by blockchain hashing or on-chain logs. The score for access control is only 54% and privacy for 30% remains secondary. Also, only 12% individuals conduct formal adversarial analysis and which indicates a lack of standardized threat modelling with a testing framework. The future papers need to focus on combining off-chain encryption and zero-knowledge, but implement it at an early stage.
- 6) **Digital-Twin Domains:** The pie results are showing a balanced focus in which patient monitoring is at 35% and IoMT device management is at 27% with high dominance. Furthermore, hospital management is at 23% and clinical simulation is only 15%. This perfect pattern reflects strong ties with precision medicine and IoT technology rather than administrative use cases.
- 7) **Quality and Validation Gaps:** From the chart, it can be seen that most studies score 4 to 6 (moderate score), which underscores that the field is conceptually rich but experimentally extremely shallow. Based on this, the high-quality studies with 30% typically integrate blockchain prototypes with realistic datasets. For example, IoMT streams had achieved better reproducibility.
- 8) **Overall Tread Synthesis:** All these charts depict a maturing but still exploratory landscape. Hence, researchers are converging on permissioned blockchain architectures for healthcare digital twins, focusing on data integrity over privacy, with increasing and uneven adoption of empirical validation. It means that future studies need to work on enhancing interoperability, standardized benchmarking, and privacy-preserving computation. Therefore, it will become simple to achieve a clinically deployable blockchain-digital twin ecosystem in the healthcare centers.

9.2 Use Cases of Healthcare Digital Twins

1. Patient Digital Twins

This domain is the most represented (e.g., Amofa et al. 2024; Suleiman et al. 2025). Patient DTs, for example, synchronise real-time bio signals from wearable sensors and clinical devices. Blockchain is used for:

- tamper-proof provenance,
- audit trails of model updates,
- Consent-driven data sharing.

However, important to consider that latency requirements for ICU or cardiac twins are evaluated empirically very rarely.

2. IoMT Device Twins

Studies such as Zheng et al. (2022) and Dai et al. (2024) tend to apply DTs to medical devices and maintenance logs among others. Meanwhile, blockchain is proposed to make sure that device lifecycle events are traceable. However, these studies do not assess the performance overhead on IoMT hardware that are resource-constrained.

3. Hospital Management Twins

Operational DTs modelling bed occupancy and workflow synchronization tend to appear in Xames & Topcu (2024). Multi-department data exchange is secured by blockchain in decentralized hospital settings and a recurring limitation is the lack of real hospital deployment data.

4. Surgical or Clinical Simulation Twins

Studies such as Suhail et al. (2022) tend to mention blockchain-led audit trails for surgical simulators, where DTs are used for modelling organ behaviour and procedural planning. Regardless, privacy and latency concerns are unsolved and are not evaluated in an experimental manner.

9.3 Strengths and Limitations of the Existing Literature

1. Strengths

- 1) Clear alignment between blockchain primitives and DT security needs. Across studies such as Suleiman et al. (2025), Amofa et al. (2024), and Dai et al. (2024), blockchain is applied consistently for improving provenance and auditability.
- 2) Emerging architectural innovations. Dual-chain and hybrid models that are proposed by Guo et al. (2021) and conceptual frameworks in Suhail et al. (2021) show higher architectural sophistication.
- 3) Integration with IoMT and edge computing. Meaningful attempts are made by Zheng et al. (2022) and Dai et al. (2024) in integrating blockchain with low-power devices and distributed DT ecosystems.
- 4) Increasing interest in governance-based DT systems. Xames & Topcu (2024) offer a mapping of healthcare DT governance challenges, which shows better conceptual clarity.

2. Limitations

- 1) Lack of empirical threat modelling. Only a minority (e.g., Amofa et al. 2024) attempt threat reasoning and most studies including Yaqoob (2020), Suhail (2022), and Suleiman (2025), depend on high-level claims without testing.
- 2) Minimal evaluation of real-world performance. Only 30% of studies (e.g., Amofa 2024; Zheng 2022) implement prototypes with latency or gas costs that are measurable, and no study assesses clinical-grade latency.
- 3) Weak privacy methodologies. In spite of concerns about GDPR/HIPAA, no included study (including Dai 2024; Suhail 2021; Xames & Topcu 2024) applies ZKPs or secure multiparty computation.
- 4) Over-reliance on conceptual and simulation-based designs. Studies such as Suhail et al. (2022) and Yaqoob (2020) are influential but are still conceptual and only a handful tend to offer real data or deployment testing.
- 5) Inconsistent evaluation metrics. Throughput and security metrics differ widely across Amofa 2024, Zheng 2022, and Dai 2024, which decreases cross-study comparability.
- 6) Insufficient interoperability considerations. None of the reviewed studies offer effective FHIR/HL7 integration pathways in spite of being important for hospital adoption.

9.4 Future Research Directions

- Future research should focus on:
- Mapping DT data structures to FHIR/HL7 standards and ensuring semantic consistency.
- Implementing practical ZKPs, securing multiparty computation, and differential privacy within DT workflows.
- Exploring DAG-based ledgers and edge-optimized consensus for low-latency DT applications.
- Enabling multi-institution DT collaboration while preserving patient privacy.
- Creating open datasets and attack taxonomies for blockchain-DT security testing.
- Carrying out controlled trials in hospitals for validating system performance and compliance.

9.5 Strengths and Limitations across the Reviewed Literature

The main strength is linked with the conceptual clarity in aligning blockchain primitives (decentralization, immutability, transparency) with digital twins (DT) security requirements (accountability, provenance, integrity). Moreover, multiple studies introduced modular frameworks integrating AI, IoMT, and edge computing that reflect on data volume constraints and awareness of scalability. However, some limitations are also present.

- Less real-world deployments: Only a few studies, less than 15% of the studies, tested blockchain-DT systems in operational healthcare settings.
- Privacy Gaps: Off-chain data storage and anonymization issues are common. Secondly, only a few studies had applied advanced privacy-preserving methods that link with homomorphic encryption, zero-knowledge proofs, and differential privacy.
- Evaluation bias: Simulation-based evaluation often misses the latency, throughput, and consensus overhead trade-off important for real-time clinical use.
- Simplistic threat Models: A lot of research assumes honest nodes and ignores adversarial networks like model inversion, data poisoning, and malicious IoT devices.

All these limitations highlighted that the field is still maturing and transitioning towards pilot implementations from a conceptual framework.

9.6 Gaps and Research Opportunities

- **Interoperability with the Health System:** Blockchain-DT platforms are required to interoperate with current standards like FHIR (Fast Healthcare Interoperability Resources) and HL7. Hence, future research needs to investigate semantic interoperability and ontology mapping for DT data anchored to EHRs.
- **Scalability and Latency Trade-Offs:** Digital twins in the ICU or surgery section require millisecond response times. However, consensus mechanisms of blockchain introduce latency. Due to this, lightweight consensus protocols like DAG-based ledgers and PBFT variants, and edge blockchain integration are the future research directions.
- **Privacy-Preserving Techniques:** Blockchain transparency must relate to the confidentiality of patients. Hence, studies must explore zero-knowledge proofs, federated DTs, and differential privacy to allow verifiable yet private computations.
- **Standardized Threat Models and Benchmarks:** Due to less consistent benchmarking, it hinders comparison across studies. It is important to implement a unified threat taxonomy for DT security by covering device layers, models, and data. For this purpose, it is reliable to establish an open benchmark dataset for DT-blockchain simulations for strengthening reproducibility.

9.7 Practical Implication

For research, the outcomes suggest that there is a need for interdisciplinary designs that integrate blockchain engineering, biomedical standards, and AI model security. For clinicians, blockchain-enabled DTs can easily increase trust and auditability in predictive models used for patient management. Lastly, for system designers, selecting a permissioned blockchain is preferable because of governance, compliance with regulations, and privacy, like HIPAA and GDPR. However, it's practical deployment demands collaboration with regulatory bodies for defining ethical guidelines and audit frameworks.

9.8 Methodological Reflection and SLR Limitations

This SLR followed PRISMA 2020 guidelines and implemented multiple academic databases to reduce publication bias. However, some constraints are still present.

- **Database Coverage:** Some industry preprints and prototypes were excluded.
- **Language Limitations:** Only English studies were selected, which ignores non-English research.

Besides these limitations, this research provides a comprehensive and up-to-date overview of the role of blockchain in DT security for healthcare.

10. Conclusion

Summing up all the discussion from above, it is concluded that blockchain technology is extremely reliable and it offers a robust foundation for enhancing transparency, security, and trust in healthcare digital twins. Moreover, its main contribution links with enabling immutable data provenance, automated policy enforcement, and decentralized access control by smart contracts. Furthermore, the review also shows persistent challenges like incomplete threat, performance bottlenecks, inadequate privacy-preserving computation, and coverage. Moreover, a lot of solutions remain at proof-of-concept and maturity that focus on simulations rather than clinical validations. Future research should focus on:

- Mapping DT data structures to FHIR/HL7 standards and ensuring semantic consistency.
- Implementing practical ZKPs, securing multiparty computation, and differential privacy within DT workflows.
- Exploring DAG-based ledgers and edge-optimized consensus for low-latency DT applications.
- Enabling multi-institution DT collaboration while pre serving patient privacy.
- Creating open datasets and attack taxonomies for blockchain-DT security testing.
- Carrying out controlled trials in hospitals for validating system performance and compliance.

Corresponding author

Hafizur Rahman
mhrahman@kfu.edu.sa

Acknowledgements

NA

Funding

NA

Contributions

Conceptualization, D.A; H.R; Methodology, D.A; H.R; Software, D.A; H.R; Validation, D.A; H.R; Formal Analysis, D.A; H.R; Investigation, D.A; H.R; Resources; D.A; H.R; Data Curation, D.A; H.R; A.A; Writing (Original Draft), D.A; H.R; Writing (Review and Editing), H.R; Visualization, H.R; Supervision; H.R; Project Administration, H.R; Funding Acquisition, H.R. All authors have read and agreed to the published version of the manuscript.

Ethics declarations

This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication

Not applicable.

Competing interests

All authors declare no competing interests

References

- [1] Amofa, S., Xiao, H. X. I. A. O. B. A.-A., J. Y., & Qi, X. (2024). Blockchain-secure patient digital twin in healthcare using smart contracts. *PLOS ONE*, *19*(2), e0286120.
- [2] Suleiman, R., Y., W., & Akshita Maradapu Vera Venkata Sai, C. W. (2025). Blockchain for security in digital twins. *Future Internet*, *17*(9), 385.
- [3] Dai, Y., X., S. M., B. G. Y. Q., L., Y., & Wu, J. (2024). Blockchain empowered access control for digital twin system with attribute-based encryption. *Future Generation Computer Systems*, *160*, 564–576.
- [4] Alghareeb, M. S., & Almaayah, M. (2025). Cyber Security Risk Management for Threats in Wireless LAN: A Literature Review. *STAP Journal of Security Risk Management*, *2025*(1), 22-58.
- [5] Machado, T. M., & Berssaneti, F. T. (2023). Literature review of digital twin in healthcare. *Heliyon*, *9*(9).
- [6] Guo, Z.-Z., Q., J.-Y., L., X.-B., R., D.-C., S., Y., & Wang, K. (2021). An intelligent maritime scene frame prediction based on digital twins technology. In *2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI)* (pp. 25–28). IEEE.
- [7] Suhail, S., O., R. J. A., S. C. S. H., & Hussain, R. M. (2022). Blockchain-based digital twins: Research trends, issues, and future challenges. *ACM Computing Surveys*, *54*(11s), 1–34.
- [8] Vallée, A. (2023). Digital twin for healthcare systems. *Frontiers in Digital Health*, *5*, 1253050.
- [9] Shankhdhar, A., & Garg, H. (2025). Blockchain-enabled secure data transmission for personalized e-healthcare and digital twin well-being. *Cluster Computing*, *28*(15).
- [10] Gupta, M., Jain, R., Kumari, M., & Narula, G. (2020). Securing healthcare data by using blockchain. In *Applications of Blockchain in Healthcare* (pp. 93–114).
- [11] Shinde, R., Patil, S., Kotecha, K., Potdar, V., Selvachandran, G., & Abraham, A. (2024). Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions. *Transactions on Emerging Telecommunications Technologies*, *35*(1).
- [12] Zarour, M., Ansari, M. T. J., Alenezi, M., Sarkar, A. K., Faizan, M., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records. *IEEE Access*, *8*.
- [13] Al-shareeda, M., & Alrudainy, H. (2026). Sustainable and Secure Energy Optimization Strategies in the Internet of Healthcare Things (IoHT). *International Journal of Cybersecurity Engineering and Innovation*, *2026*(1).
- [14] Ghosh, P. K., R., M. H. K., S., A. H., & Chakraborty, A. (2023). Blockchain application in healthcare systems: A review. *Systems*, *11*(1), 38.

- [15] Alrajeh, M., Almaiah, M., & Mamodiya, U. (2026). Cyber Risk Analysis and Security Practices in Industrial Manufacturing: Empirical Evidence and Literature Insights. *International Journal of Cybersecurity Engineering and Innovation*, 2026(1).
- [16] Ibrahim, A., Kadhim, A. F., Hamzah, A. E., & Al-Shareeda, M. A. (2026). A Secure and Scalable IoT Home Automation Architecture with Web and Biometric Control. *International Journal of Cybersecurity Engineering and Innovation*, 2026(1).
- [17] Wells, K., & Littell, J. H. (2009). Study quality assessment in systematic reviews of research on intervention effects. *Research on Social Work Practice*, 19(1), 52–62.
- [18] Sterne, J. A., Hernán, M. A., McAleenan, A., Reeves, B. C., & Higgins, J. P. (2019). Assessing risk of bias in a non-randomized study. In *Cochrane Handbook for Systematic Reviews of Interventions* (pp. 621–641).
- [19] Whiting, P., Savović, J., & Higgins, J. P. (2016). ROBIS: A new tool to assess risk of bias in systematic reviews was developed. *Journal of Clinical Epidemiology*, 69, 225–234.
- [20] Lundh, A., & Gøtzsche, P. C. (2008). Recommendations by Cochrane Review Groups for assessment of the risk of bias in studies. *BMC Medical Research Methodology*, 8(1).
- [21] Talib, A. H., AL-Nakkash, A. H., Wadday, A. G., Abed, A. A., & Al-Shareeda, M. A. (2026). Real-Time Spectrum Sensing on an RTL-SDR-Based IoT Platform. *International Journal of Cybersecurity Engineering and Innovation*, 2026(1).
- [22] Yaqoob, I., J., M. U. R., O., M. I., & Salah, K. (2020). Blockchain for digital twins: Recent advances and future research challenges. *IEEE Network*, 34(5), 290–298.
- [23] Suhail, S., & Hussain, R. J. a. C. S. H. (2021). Trustworthy digital twins in the industrial internet of things with blockchain. *IEEE Internet Computing*, 26(3), 58–67.
- [24] Zheng, Q., S., Y. P. D., C., M., & Wang, J. (2022). Blockchain-based trustworthy digital twin in the Internet of Things. In *2022 International Conference on Information Processing and Network Provisioning (ICIPNP)* (pp. 152–155). IEEE.
- [25] Xames, M. D., & Topcu, T. G. (2024). A systematic literature review of digital twin research for healthcare systems: Research trends, gaps, and realization challenges. *IEEE Access*, 12, 4099–4126.