Open Access Library Journal
2026, Volume 13, e16050
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Advancing Identity-Centric Zero-Trust Security for Critical Infrastructure: A Systematic Review and Evidence Map of Continuous Authentication, Adaptive Authorization, and Post-Authentication Threat Detection

Samuel Dushimimana Shyaka[1], Collin Arnold Kabwama[2]

[1]College of Engineering, Carnegie Mellon University Africa, Kigali, Rwanda
[2]Department of Computer Science, Maharishi International University, Fairfield, IA, USA
Email: sdushimi@alumni.cmu.edu

How to cite this paper: Shyaka, S.D. and Kabwama, C.A. (2026) Advancing Identity-Centric Zero-Trust Security for Critical Infrastructure: A Systematic Review and Evidence Map of Continuous Authentication, Adaptive Authorization, and Post-Authentication Threat Detection. *Open Access Library Journal*, **13**: e16050.
https://doi.org/10.4236/oalib.1116050

Received: September 20, 2026
Accepted: November 20, 2026
Published: November 23, 2026

Copyright © 2026 by author(s) and Open Access Library Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

Zero-trust architecture replaces location-based trust with explicit, context-sensitive decisions, a shift that matters most in critical infrastructure, where IT, operational technology, industrial IoT, remote access, and cloud services coexist. This PRISMA 2020 systematic review asks what evidence is collected after an identity is authenticated, how it becomes trust or risk, and how the system then changes the identity's ability to act. Three predeclared Semantic Scholar queries (2020 to September 2026) identified 1037 records and yielded 425 included studies, 196 in critical-infrastructure contexts; studies were coded against a seven-stage identity lifecycle, and 70 core studies received an evidence-maturity appraisal. Behavioural and device-level continuous authentication, physical unclonable functions, contextual trust scoring, federated learning, and graph-based detection have advanced strongly, but evidence is weakly coupled to safe, timely authorization change: 46 studies detect without enforcing, 31 revoke sessions, 13 restrict commands, 30 address safety, and one reports time-to-constrain. The article proposes an Identity Risk State feedback architecture and an evaluation framework centred on time-to-constrain, residual privilege, false-revocation cost, safety, privacy, and policy latency.

Subject Areas

Computer Science, Information Security

Keywords

Zero Trust, Identity-Centric Security, Critical Infrastructure, Continuous Authentication, Continuous Authorization, Post-Authentication Threat Detection, Industrial Control Systems, Industrial IoT, Adaptive Access Control, Systematic Review

1. Introduction

Critical-infrastructure operators now combine enterprise information technology (IT) with operational technology (OT), industrial Internet of Things (IIoT) devices, cloud services, and remote engineering access, multiplying identities: employees, contractors, service accounts, workloads, gateways, controllers, and sensors. Treating a successful login or an internal network location as durable evidence of trust is poorly matched to this reality.

NIST SP 800-207 defines zero trust as granting no implicit trust on the basis of location or ownership, deciding access per resource under dynamic policy, and continually monitoring system state [1]; SP 800-207A extends this to cloud-native services [2], and the CISA Zero Trust Maturity Model places identity first among five pillars, progressing from static to continuous validation [3]. Authentication establishes that an identity claim is credible at a point in time; it does not guarantee that the actor controlling a session remains legitimate, that the endpoint remains uncompromised, or that later actions remain consistent with the actor's role and with the physical process being controlled. Session hijacking, token theft, insider misuse, and malicious use of legitimate credentials therefore constitute a post-authentication problem.

The relevant research is spread across continuous authentication (CA) [4]-[6], user and entity behaviour analytics (UEBA) and insider-threat detection [7], continuous device authentication for IoT and IIoT [8]-[10], and industrial zero trust with cyber-physical telemetry, gateway enforcement, and federated learning [11]-[13]. Existing reviews map zero-trust architectures across domains [14], trust-scoring algorithms [15], and zero trust for Industry 5.0 and IIoT [16], but none makes the complete post-authentication identity lifecycle the unit of analysis or quantifies how often the literature closes the loop between detection and enforcement.

This review asks: after an identity has been authenticated and granted access, what evidence is collected, how is it converted into trust or risk, and how does the system change the identity's ability to act? It contributes an identity-centric lifecycle taxonomy; an evidence map of 425 studies; a quantified analysis of the detection-to-enforcement gap; an evidence-maturity appraisal of 70 core studies; an Identity Risk State (IRS) feedback architecture; and an outcome-oriented research agenda. Seven research questions address how identity-centric zero trust is operationalised (RQ1), which signals reassess identity confidence (RQ2), which models convert them into trust or risk (RQ3), how estimates become authorization

changes (RQ4), which approaches address post-authentication compromise (RQ5), how strong the evidence is under critical-infrastructure constraints (RQ6), and which gaps should set the agenda (RQ7).

2. Systematic Review Methodology

2.1. Scope, Sources, and Search Strategy

The review follows PRISMA 2020 [17] and software-engineering review guidance [18]. The window was 1 January 2020, the year SP 800-207 appeared, to 3 September 2026. The population was human and non-human identities accessing digital or cyber-physical resources; interventions were continuous authentication, attestation, adaptive authorization, dynamic trust evaluation, UEBA and insider-threat detection, session-risk analysis, and automated restriction or revocation; and the context was critical infrastructure (ICS and OT, IIoT, cyber-physical systems, smart grids, 5G/6G edge, healthcare) plus directly transferable zero-trust mechanisms. Records were retrieved on 6 September 2026 from the Semantic Scholar Academic Graph bulk search interface, restricted to computer science, using three predeclared queries (Table 1): a main query, a query without the infrastructure block to capture transferable mechanisms, and a query without the zero-trust block to capture unlabelled infrastructure mechanisms. Backward citation chasing supplied further candidates. Queries used the Semantic Scholar paper bulk-search endpoint (/graph/v1/paper/search/bulk), which matches titles and abstracts, filtered to field of study = Computer Science and publication dates 1 January 2020 to 3 September 2026; every result page was retrieved by following the continuation token until none remained. Records were keyed by Semantic Scholar paper identifier and deduplicated by DOI and, without a DOI, by normalised title (lowercased, punctuation and whitespace removed). Query strings, identifiers, and decisions are recorded in supplementary table S1.

Table 1. Predeclared queries and yields (Semantic Scholar bulk search syntax; "+" denotes AND, "|" denotes OR).

Query	Blocks	Records	Included
Q1 main	("zero trust" | "zero-trust") + (identity | "continuous authentication" | "continuous verification" | "continuous authorization" | "adaptive authorization" | "risk-adaptive access control" | "dynamic trust" | "trust score" | "trust evaluation" | "behavior analytics" | "insider threat" | "session hijacking") + ("critical infrastructure" | "industrial control" | ICS | SCADA | "operational technology" | IIoT | "industrial internet of things" | "smart grid" | "cyber physical" | "cyber-physical" | "industrial IoT")	157	56
Q2 (no infrastructure block)	("zero trust" | "zero-trust") + ("continuous authentication" | "continuous verification" | "continuous authorization" | "risk-adaptive access control" | "trust score" | "trust evaluation" | "dynamic trust" | "session hijacking")	777	374
Q3 (no zero-trust block)	("continuous authentication" | "insider threat detection" | "behavior analytics" | "adaptive access control" | "dynamic access control") + ("critical infrastructure" | "industrial control system" | SCADA | "operational technology" | IIoT | "industrial internet of things" | "smart grid")	103	41
Total before deduplication		1037	414 (unique)

2.2. Eligibility, Screening, and Coding

Eligible records were peer-reviewed papers, authoritative standards, or reviews in English that described at least one continuous or post-authentication identity mechanism (continuous authentication, dynamic trust used for access decisions, adaptive authorization, identity- or session-level detection, or restriction and revocation) with evaluable content. Excluded were one-time authentication or authorization only, zero-trust work limited to segmentation, SDN, encryption, or consensus without an identity mechanism, non-transferable consumer settings, preprints, theses, patents, and opinion pieces. Transferability from cloud, enterprise, and general settings was judged on the mechanism: a study was retained when its mechanism uses session, device, or behavioural evidence an infrastructure operator could also collect to reach a trust or access decision, and excluded when it depends on consumer-specific signals. This unvalidated reviewer judgement is why transferable studies are counted separately from the 196 critical-infrastructure studies, to which the appraisal is confined. Records were deduplicated, screened on title and abstract, and assessed for eligibility with a reason code for each exclusion; rule-assisted first-pass classification was reviewed decision by the author, and 35 records without an abstract were assessed from the title and, where known, the full text (Figure 1). Each study was coded for context, identity type, lifecycle stages, continuous signal, model family, enforcement action, highest evaluation level, constraints addressed, metrics, findings, and limitations (abstract level for all studies, full text for core studies); the coded extraction for all 425 studies is given in supplementary table S2. Outcome heterogeneity precluded pooling.

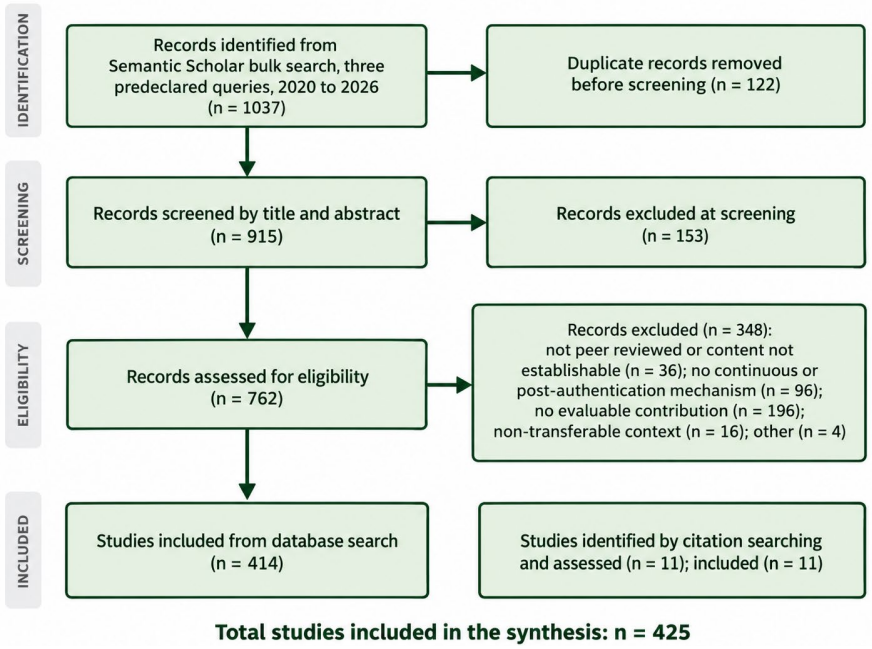

Figure 1. PRISMA 2020 flow of identification, screening, eligibility assessment, and inclusion.

2.3. Quality and Applicability Appraisal

The 70 core studies were those set in a critical-infrastructure context that report an evaluation beyond simulation alone and specify an enforcement action, plus three foundational industrial studies from citation searching (LCDA [8], FedZTA [11], and the gateway architecture of Zanasi *et al.* [12]). Formal security analysis counts as evaluation beyond simulation under this definition, and 20 core studies are coded with formal analysis as their highest level; the coded level is the single highest level a study reports, so a study described as using formal analysis and simulation is coded as formal. Of the 67 database-retrieved core studies, 64 satisfy both criteria as coded. Three are exceptions that were retained on the strength of their full text: PUFDCA [9], a protocol verified with an automated tool but with no enforcement action coded; the cyber-physical architecture of Feng and Hu [19], evaluated by simulation with explicit attack models; and ZT-RIASE [13], a fully specified attestation protocol with security and overhead analysis whose abstract reports neither item. They are identified in the **Appendix** and should be read as exceptions to the selection rule. Six domains were rated 0 (not addressed), 1 (partially), or 2 (clearly addressed): Q1 threat model, Q2 reproducible description, Q3 empirical or formal validation, Q4 realistic workload or testbed, Q5 baselines with meaningful metrics, and Q6 critical-infrastructure applicability. Totals of 10 to 12 indicate high evidence maturity, 6 to 9 moderate, and 0 to 5 limited. Domain scores and a justification for each core study are given in supplementary table S3.

3. Conceptual Framework: The Post-Authentication Identity Lifecycle

Identity, not network location or product category, is the organising unit. Seven stages are distinguished (**Figure 2**, **Table 2**): stages 1 to 3 are point-in-time decisions at session establishment, and stages 4 to 7 operate during the active session and are the focus of this review.

Table 2. Lifecycle stages, security questions, mechanisms, evidence, and policy consequences.

Stage	Security question	Typical mechanisms	Evidence produced	Policy consequence
1 Identity establishment	Who or what is the entity?	Federation, certificates, PUF, workload identity	Identity assurance	Eligibility for policy
2 Initial authentication	Is the claim credible now?	MFA, cryptographic challenge, biometrics, attestation	Authentication confidence	Session establishment
3 Initial authorization	What may it do now?	RBAC, ABAC, least privilege, policy engine	Permission scope	Bounded access
4 Continuous authentication	Is it still the same legitimate entity?	Behavioural biometrics, context, device and location checks, channel properties	Updated identity confidence	Maintain or step up
5 Post-authentication detection	Is behaviour consistent and non-malicious?	UEBA, anomaly and graph models, session and network analytics	Behavioural threat evidence	Investigate or restrict
6 Dynamic trust reassessment	Does accumulated evidence still justify trust?	Risk score, Bayesian, machine-learning, fuzzy, or federated models	Identity Risk State	Risk band changes
7 Adaptive authorization and revocation	What may it do now?	Token and privilege adjustment, command restriction, isolation, revocation	Enforced state	Constrain or terminate

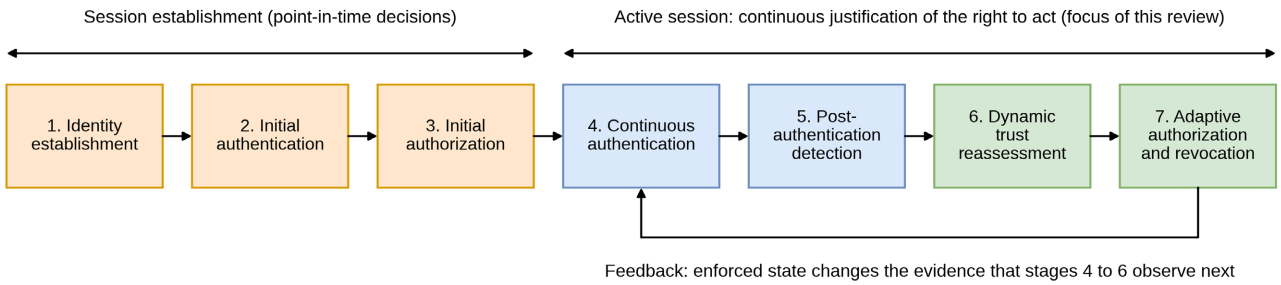

Figure 2. The seven-stage post-authentication identity lifecycle. Stages 4 to 7 form a feedback loop in which enforced state changes the evidence observed next.

4. Results: Landscape of the Evidence

Search Results and Study Characteristics

The queries returned 1037 records; after removing 122 duplicates, 915 were screened and 153 excluded, and of 762 assessed for eligibility 348 were excluded, most often for lack of an evaluable contribution (196) or of a continuous identity mechanism (96) (**Figure 1**). Citation searching added 11 studies to the 414 retained, including LCDA [8], FedZTA [11], the gateway architecture of Zanasi *et al.* [12], and surveys [5]-[7] [16] [20], giving 425 included studies.

Of these, 306 (72 percent) appeared in 2025 or 2026. By context, 196 (46 percent) are set in critical infrastructure (IIoT 50, 5G/6G edge 35, cyber-physical systems 32, ICS and OT 27, smart grid 27, healthcare 25), 115 in cloud or enterprise settings, and 82 present general mechanisms; 32 are reviews or standards. Identity type is mixed in 205 studies, device-only in 101, human-only in 88, and workload or service in 31. Hybrid architectures (97) and machine or deep learning (88) are the most common trust-evaluation families, followed by rule or threshold scoring (75), graph models (48), federated learning (29), blockchain (28), Bayesian models (19), reinforcement learning (13), and fuzzy logic (5) (**Figure 3**). Continuous signals are behavioural in 232 studies, contextual in 185, network telemetry in 111, device posture in 46, behavioural biometrics in 31, process or physical state in 29, PUF or channel properties in 22, and crypto-behavioural attestation in 12.

Dynamic trust reassessment (295 studies), adaptive authorization or revocation (282), and continuous authentication (272) are widely addressed, and post-authentication detection by 175 (**Figure 4**). Enforcement is less varied than the models that drive it: 182 studies adjust privileges, 93 isolate or segment, 30 trigger step-up authentication, 31 revoke sessions, and 13 restrict individual commands, while 46 detect without enforcing and 50 specify no action. These categories record the action a study describes; abstract-level coding cannot separate implemented and evaluated actions from proposed ones, so they are upper bounds on demonstrated enforcement. Within the core set, 48 of 70 studies specify an enforcement action and evaluate the mechanism on a testbed, prototype, or real dataset; 20 rely on formal analysis. Simulation is the highest evaluation level in 165 studies, including 91 of the 196 critical-infrastructure studies (**Figure 5**); 68

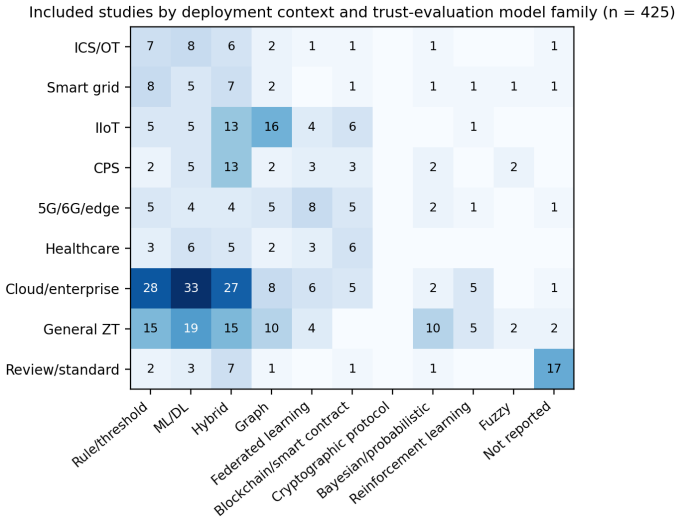

Figure 3. Included studies by deployment context and trust-evaluation model family.

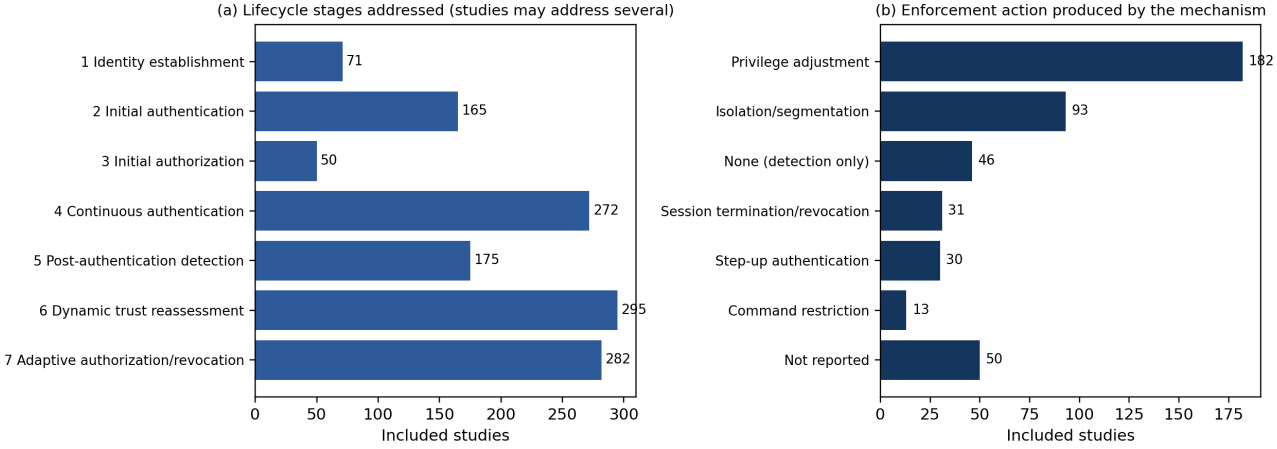

Figure 4. (a) Lifecycle stages addressed and (b) enforcement action produced by the mechanism.

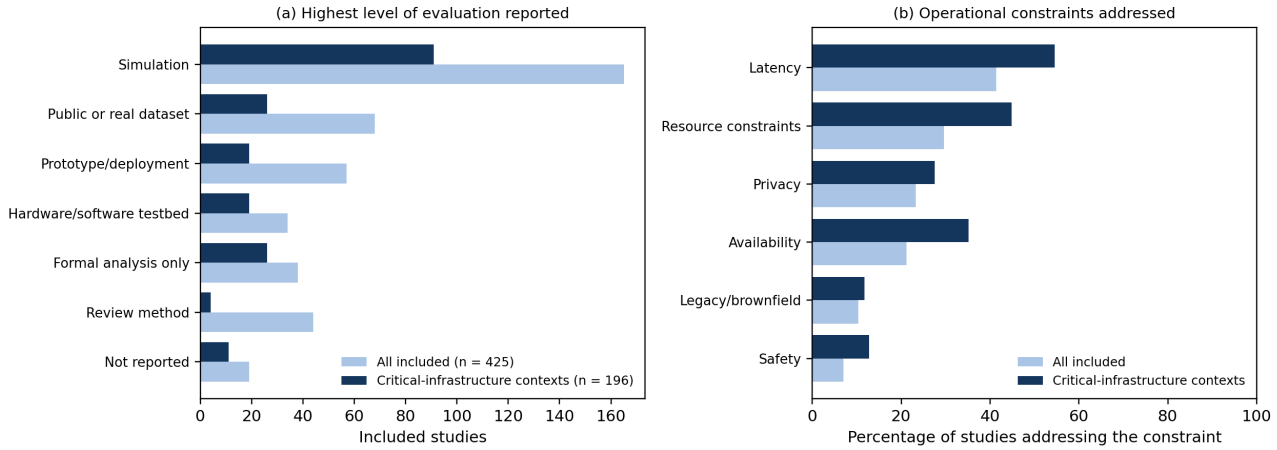

Figure 5. (a) Highest level of evaluation reported and (b) operational constraints addressed, for all included studies and for the critical-infrastructure subset.

use a public or real dataset, 57 a prototype or deployment, 34 a testbed, and 38 formal analysis alone. Latency is the most addressed constraint (176), then resource limits (126), privacy (99), availability (90), legacy compatibility (44), and safety (30). Accuracy (129) and latency (82) dominate the metrics; false-positive rates appear in 39 studies, revocation measures in 3, and time-to-constrain in one. In short, the literature reasons about trust far more often than it acts on it.

5. Continuous Authentication (RQ2 and RQ3)

Continuous authentication extends access control beyond login [4]; surveys stress the balance of security, privacy, and usability and show that human-centred methods do not transfer to constrained devices without modification [5] [6]. Abba *et al.* reported multimodal behavioural trust scoring for remote healthcare work with sub-3 ms inference [21]. Behavioural signals drift and are affected by gloves, shared consoles, fatigue, and emergency operation, and collection creates privacy risk that homomorphic feature matching can reduce [20].

Non-human identity requires different evidence. LCDA derives changing session keys from channel properties for lightweight device-to-device CA [8]; PUFDCA combines physical-unclonable-function (PUF) identity with continuous location and channel checks [9]; Wan *et al.* add three-factor user verification for IIoT [10]; Meng *et al.* remove the trusted authority through Byzantine fault-tolerant consensus [22]. Hardware-rooted work adds TPM attestation of PLC-connected devices [23], eSIM re-attestation for MQTT [24] and the 5G core [25], and temperature-compensated CAN-bus fingerprints [26], while ZT-RIASE replaces repeated public-key operations with runtime attestation from token-use regularity, command consistency, timing, and energy deviation [13]. CA is thus moving from repeated proof of a static secret toward inference from an evidence stream, yet 99 of 272 CA studies describe no authorization or revocation consequence.

6. Continuous and Risk-Adaptive Authorization (RQ4)

Authorization is the decisive control plane: continuous verification adds little if permissions do not change when risk rises [1] [2]. Trust algorithms remain fragmented and weakly standardised [15], and the same numerical score means very different things for an email account and a safety-critical controller. Among studies that specify how risk changes permitted action, Ghnaimat *et al.* re-derive risk-proportional decisions with traceable defeasible-logic rationales [27]; Saha *et al.* implement decentralised risk-adaptive control for industrial data sharing with 24 percent lower latency than a centralised baseline [28]; Feng *et al.* combine hidden-policy attribute-based encryption with smart-contract trust to penalise malicious IIoT nodes [29]; and federated designs exclude clients whose trust falls [30]. In industry, FedZTA fuses subject, object, cyber, and physical information through asynchronous federated learning [11]; Feng and Hu's cyber-physical architecture raises false-data-injection detection by more than 31 percent [19]; and Han *et al.*

deployed dynamic trust evaluation for remote substation maintenance [31]. Because an authenticated identity may request a command that is unsafe for the current process state, authorization should be both identity-aware and process-aware.

The literature supports graded responses (more logging, shorter token lifetime, step-up authentication, privilege narrowing, command restriction, supervised operation, isolation, revocation) rather than a single allow-or-deny threshold, yet step-up appears in only 30 studies, revocation in 31, and command restriction in 13, almost all in platooning, drone, or fieldbus settings [26] [32]. Given OT availability and safety needs, this scarcity is one of the clearest findings of the review.

7. Post-Authentication Threat Detection (RQ5)

Post-authentication detection addresses session hijacking, stolen tokens, compromised endpoints, malicious insiders, privilege misuse, and lateral movement, which is why multifactor authentication is necessary but insufficient. Graph methods suit the relational nature of identity risk [7], as in fraud detection with graph attention networks and graph reinforcement learning [33] [34], where language models are also emerging [35]. These fraud studies are cited as methodological analogues only: transaction graphs have abundant confirmed labels, no physical process, and no safety cost of a false positive, so their results do not establish detection performance for post-authentication threats in critical infrastructure. Rguig and Housni converted attention weights into device trust scores [36]; Hassan *et al.* unified zero trust, SIEM, SOAR, and UEBA with interpretable models that trigger responses [37]; digital twins support anomaly detection in industrial cyber-physical systems [38]; and a Bayesian and transformer trust model raised inhibition of lateral movement from building automation into hydropower monitoring networks by more than 150 percent on a high-fidelity testbed [39]. Because legitimate emergencies are anomalous and attackers mimic normal behaviour, the useful output is evidence that shifts confidence in continued access, not an anomaly label. The main weakness is incomplete coupling: 41 of 175 detection studies stop at detection: 33 are coded as detection only and 8 specify no enforcement action. The 46 detection-only studies reported in Section 4.1 are counted across all 425 studies; 33 of them are these stage-5 detection studies and the other 13 are not coded to the detection stage, and few measure how long a compromised identity retains privilege or which legitimate operations a response disrupts.

8. Critical-Infrastructure Applicability (RQ6)

8.1. Operating Constraints

Controls must coexist with availability, safety, and long asset lifecycles, and brownfield OT devices often cannot run agents or tolerate frequent handshakes. Enforcement therefore sits at gateways, jump hosts, or remote-access brokers, as in the ICS prototype [40] and brownfield gateway architecture [12] of Zanasi *et al.*, the edge architecture of Lei *et al.* [41], and embedded and containerised edge

implementations [42] [43]. A remote vendor should reach only one asset during an approved window, as implemented for substations [31] and through task-based just-in-time privileges for drone swarms [44]; a controller may hold a valid identity yet issue an unexpected command pattern, the gap addressed by fingerprinting [26], attestation [23], and network-based identification [45]. Safety makes false positives asymmetric: low-confidence anomalies may justify observation or step-up, stronger evidence command restriction or supervised operation, and only high, safety-consistent confidence isolation or revocation. Only 30 studies address safety, mostly in platooning and unmanned systems, where Mamun and Picone proved monotonicity of a risk model while eliminating accepted malicious control packets [32].

8.2. Core Evidence and Appraisal

Table 3 presents representative core studies, and **Appendix** (Table A1) reports the appraisal of all 70. Twenty-five reached the high band, 37 moderate, and 8 limited. Empirical or formal validation scored highest (mean 1.80 of 2) and critical-infrastructure applicability was frequently addressed (1.60), whereas realistic workload or testbed scored lowest (1.07), followed by threat modelling (1.26) and baselines and metrics (1.24). The review extends the industrial taxonomy of Akhmetkaliyev *et al.* [16] by treating the gateway as one actuator in an identity-risk feedback loop and showing how rarely that loop is closed and measured.

Table 3. Representative core studies by context.

Study	Context	Identity	Continuous evidence	Trust or detection model	Enforcement	Evaluation
Shah *et al.* 2021, LCDA [8]	IIoT/critical	Device	Channel and session properties	Lightweight cryptographic protocol	Session key renewal and termination	Formal analysis, simulation
Alshomrani and Li 2022, PUFDCA [9]	IoT	Device	PUF plus location and channel	Protocol verification	Maintain or reject	Formal analysis, performance
Zanasi *et al.* 2022 [40]	ICS	Mixed	Identity and posture at gateway	Rule-based policy	Isolation and segmentation	Industrial prototype
Feng and Hu 2023 [19]	Industrial CPS	Mixed	Cyber and physical layer state	Hybrid cross-layer model	Privilege adjustment	Simulation with attack models
Zanasi *et al.* 2024 [12]	Brownfield IIoT	Mixed	Device posture, network telemetry	Rule-based policy at gateway	Isolation and segmentation	Industrial testbed
Ge and Zhu 2024, GAZETA [46]	5G IoT	Mixed	Interdependent trust evidence	Markov game equilibrium	Step-up authentication	Formal analysis, case study
Saha *et al.* 2024, AALMOND [28]	IIoT	Mixed	Context and behaviour	Blockchain risk-adaptive control	Privilege adjustment	Prototype deployment
Poduvu *et al.* 2024, Arculus [44]	Tactical edge	Mixed	Task and mission context	Task-based access control	Just-in-time grant and revocation	Drone-swarm testbed
Lv *et al.* 2025, FedZTA [11]	ICS	Mixed	Subject, object, cyber, physical	Asynchronous federated learning	Access decision	Industrial-oriented evaluation

Continued

Wan *et al.* 2025 [10]	IIoT	User and device	PUF plus location	Cryptographic protocol	Continuous verification and termination	Formal analysis, performance
Zhang *et al.* 2025, OMATE-ZT [47]	IIoT	Mixed	Multi-attribute behaviour	FastKAN trust evaluation	Privilege adjustment	Real industrial dataset
Han *et al.* 2025 [31]	Substation O&M	Human	Session context	Dynamic trust evaluation	Privilege adjustment	Real substation deployment
Lv *et al.* 2025, TADAS [26]	Fieldbus	Device	Signal fingerprints	Temperature-compensated matching	Command restriction	Real CAN-bus testbed
Verma *et al.* 2026, ZT-RIASE [13]	Smart IIoT	Device	Crypto-behavioural attestation	Runtime identity attestation	Fast revocation	Protocol analysis, simulation
Lu *et al.* 2026 [39]	Hydropower ICS	Mixed	Network and behavioural evidence	Bayesian and transformer trust	Micro-segmentation	High-fidelity cyber-physical testbed
Mamun and Picone 2026 [32]	Vehicle platoon	Mixed	Control-plane evidence	Risk model with monotonicity proof	Slice isolation, priority adjustment	Simulation and proof
Qu *et al.* 2026 [48]	UAV systems	Device	Acoustic verification	Beta-distribution trust	Isolation, privilege adjustment	Testbed
Ramzi Rashid *et al.* 2026, Edge-ZTA [49]	IoT edge	Device	Federated autoencoder evidence	Hybrid with SDN policy	Dynamic micro-segmentation	Hybrid physical and virtual testbed

9. Proposed Identity Risk State Feedback Architecture

In the proposed architecture, continuously collected evidence updates a session-specific Identity Risk State that authorization policy explicitly consumes (**Figure 6**). The IRS is resource-aware, time-varying, explainable, and bounded by safety policy.

$$IRS(t) = f\{IA, AU(t), DP(t), BH(t), NW(t), CX(t), CP(t), RS, H(t)\} \quad (1)$$

where IA is identity assurance, AU ongoing authentication evidence, DP device or workload posture, BH behavioural evidence, NW network and session evidence, CX context, CP cyber-physical or process evidence, RS resource sensitivity, and H recent history. The function f may be rules, probabilistic inference, fuzzy logic, machine learning, federated learning, or a hybrid, all represented in the corpus (**Figure 3**); the critical requirement is calibrated linkage to policy. Seven design steps follow: (1) Establish authoritative human, device, service, and workload identities and their delegation chains; (2) Perform strong initial authentication and hardware-rooted attestation where available [23] [25]; (3) Grant minimum task privilege [44]; (4) Collect evidence at a rate suited to risk, device capability, and process timing [8] [13]; (5) Fuse evidence into an IRS with explicit uncertainty; (6) Map IRS bands and safety state to graduated actions (observe, challenge, shorten, restrict, supervise, isolate, revoke); (7) Record overrides, incidents, false revocations, and outcomes for recalibration.

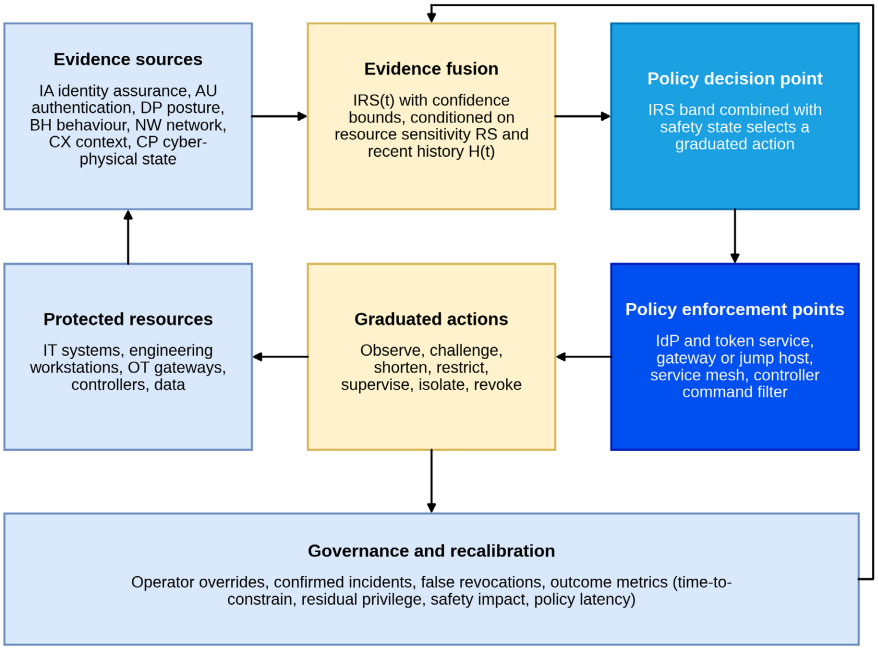

Figure 6. Identity Risk State feedback architecture. Evidence is fused into a session-specific risk state with confidence bounds; the policy decision point maps risk band and safety state to graduated actions; enforcement changes the evidence observed next; and governance recalibrates the loop from outcomes.

10. Research Gaps (RQ7)

Detection-to-authorization coupling. Forty-six studies detect without enforcing, enforcement is rarely shown to be implemented and evaluated, and one measures time-to-constrain; policy consequence should become a first-class outcome. *Machine identity*. Only 31 studies concentrate on workload or service identities, which should be unified with human authorization and delegation. *Brownfield validation*. Gateway designs are promising [12] [40] [42], but only 44 studies address legacy compatibility; field validation should cover legacy protocols, mixed vendors, intermittent connectivity, maintenance windows, and failover. *Cyber-physical evidence*. Only 29 studies use process or physical state [11] [19] [39], and hybrid quantum-classical anomaly detection over sensor networks is one emerging source [50]. *Safety-aware enforcement*. Only 30 studies address safety; policy should encode safe states, command criticality, and supervised operation, preferring command-level restriction [26] [32] to termination where the process permits.

Privacy. Federated analytics [11] [51], encrypted-domain matching [20], blockchain-based federated identity management for cross-sector trust [52], minimisation, and local processing require evaluation alongside security. *Drift and adversarial adaptation.* Trust models should be tested under benign drift, mimicry, poisoning, replay, and telemetry loss; game-theoretic [46] [53] and Byzantine-resilient [30] designs are early responses, generative adversarial modelling of infrastructure vulnerabilities [54] can synthesise test conditions, and graph-based fraud de-

tectors that lose most of their accuracy under gradient-based evasion unless adversarially trained [55] indicate the scale of the problem, although that finding comes from financial data and has not been reproduced on infrastructure identity telemetry. *Outcome metrics and governance*. Studies need time-to-constrain, residual privilege, false-revocation cost, safety impact, policy latency, and operator burden, and operators need evidence provenance, uncertainty, rationale, and auditable overrides, as defeasible-logic designs begin to offer [27].

11. Proposed Evaluation Framework for Future Studies

Table 4 specifies a minimum reporting set that connects detection quality to operational security outcomes and makes mechanisms now evaluated with incompatible metrics comparable.

Table 4. Evaluation framework for identity-centric zero-trust studies in critical infrastructure.

Dimension	Minimum metric	Why it matters	Example question
Identity assurance	FAR, FRR, EER, or protocol security properties	Measures authentication quality	Can an impostor or session takeover persist?
Detection	Precision, recall, F1 at realistic base rates; calibration	Controls false alerts and missed compromise	Does risk probability mean what it claims?
Policy response	Time-to-constrain and time-to-revoke	Links detection to protection	How long does risky privilege persist?
Residual exposure	Actions or privileges available after compromise begins	Measures actual security consequence	What can the attacker still do?
Availability	Added latency, downtime, failure behaviour	OT cannot ignore service continuity	Does enforcement disrupt control?
Safety	Unsafe-action prevention and false-revocation impact	Security actions affect the physical process	Can the response itself create a hazard?
Privacy	Raw data exposure, retention, inference leakage	Monitoring observes users and devices	What sensitive information is revealed?
Robustness	Performance under drift, evasion, poisoning, telemetry loss	Deployments change and are attacked	Does trust remain reliable under adaptation?
Interoperability	Protocols, vendors, and asset classes covered	Brownfield deployment is heterogeneous	Can the method span mixed OT estates?
Human factors	Step-up frequency, override burden, operator workload	Operators must work under pressure	Does security become operationally unusable?

12. Discussion

Identity-centric zero trust is better represented as a feedback-control problem than as an authentication stack. Authorization is the actuator; when it is disconnected from the evidence stream, the architecture observes continuously but does not enforce continuously: trust reassessment is addressed by 295 studies, but revocation by 31, command restriction by 13, safety by 30, and time-to-constrain by one. Because a legitimate insider can act maliciously without failing verification and a hijacked session may initially imitate normal behaviour, authentication con-

fidence and behavioural risk must be fused and conditioned on device, resource, and operational context.

The IRS architecture is deliberately algorithm-agnostic: every model family appears in the corpus, and high-maturity examples exist in several (**Appendix**). Blockchain-recorded policy enforcement and anomaly response [56] illustrate one way to remove the central policy engine as a single point of failure, although their latency against control loops remains to be measured. Caution is warranted, since many recent studies are simulation-only papers reporting accuracy above 95 percent on generic intrusion datasets; core studies combining explicit threat models, realistic testbeds, and outcome metrics [11] [12] [26] [31] [39] [44] should serve as reference points.

13. Limitations

Relevant work may use continuous verification, adaptive access, or insider-threat vocabulary without the zero-trust label, and records came from a single index; supplementary queries and citation searching mitigate but cannot eliminate this risk. Screening was completed by a single reviewer with rule-assisted classification and a full decision record. Coding was at abstract level for most studies, so counts are lower bounds and proposed enforcement cannot be separated from evaluated enforcement outside the core set; transferability of non-infrastructure mechanisms was judged by the reviewer and not tested; meta-analysis was inappropriate given heterogeneous outcomes; and the corpus is dominated by recent simulation-level studies.

14. Conclusion

For critical infrastructure, the decisive advance is not stronger or more frequent authentication but the ability to collect evidence continuously, reassess whether a human or machine identity remains trustworthy for a particular resource and action, and translate that reassessment into calibrated, safe, and timely authorization changes. The 425 studies reviewed supply strong building blocks, from behavioural biometrics and hardware attestation to federated trust evaluation and graph-based detection. The remaining challenge is end-to-end validation on realistic brownfield workloads with metrics for residual privilege, time-to-constrain, availability, safety, privacy, and operator burden.

Author Contributions

Samuel Dushimimana Shyaka and Collin Kabwama: Conceptualization, Methodology, Investigation, Data curation, Formal analysis, Visualization, Writing (original draft), Writing (review and editing).

Data Availability

No new primary data were created. The search log, screening decisions with rea-

son codes, coded extraction table for all 425 studies, and appraisal scores are provided as supplementary tables S1 to S3, which are not printed in the article but are supplied as a separate supplementary workbook available at https://zenodo.org/records/23285325.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) Zero Trust Architecture. National Institute of Standards and Technology.

[2] Chandramouli, R. and Butcher, Z. (2023) A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments. National Institute of Standards and Technology (U.S.).

[3] Cybersecurity and Infrastructure Security Agency (2023) Zero Trust Maturity Model, Version 2.0. CISA. https://www.cisa.gov/zero-trust-maturity-model

[4] Junquera-Sánchez, J., Cilleruelo, C., De-Marcos, L. and Martinez-Herráiz, J. (2021) Access Control beyond Authentication. *Security and Communication Networks*, **2021**, 1-11. https://doi.org/10.1155/2021/8146553

[5] Baig, A.F. and Eskeland, S. (2021) Security, Privacy, and Usability in Continuous Authentication: A Survey. *Sensors*, **21**, Article 5967. https://doi.org/10.3390/s21175967

[6] Al-Naji, F.H. and Zagrouba, R. (2020) A Survey on Continuous Authentication Methods in Internet of Things Environment. *Computer Communications*, **163**, 109-133. https://doi.org/10.1016/j.comcom.2020.09.006

[7] Gong, Y., Cui, S., Liu, S., Jiang, B., Dong, C. and Lu, Z. (2024) Graph-Based Insider Threat Detection: A Survey. *Computer Networks*, **254**, Article 110757. https://doi.org/10.1016/j.comnet.2024.110757

[8] Shah, S.W., Syed, N.F., Shaghaghi, A., Anwar, A., Baig, Z. and Doss, R. (2021) LCDA: Lightweight Continuous Device-to-Device Authentication for a Zero Trust Architecture (ZTA). *Computers & Security*, **108**, Article 102351. https://doi.org/10.1016/j.cose.2021.102351

[9] Alshomrani, S. and Li, S. (2022) PUFDCA: A Zero-Trust-Based IoT Device Continuous Authentication Protocol. *Wireless Communications and Mobile Computing*, **2022**, Article 6367579. https://doi.org/10.1155/2022/6367579

[10] Wan, T., Shi, B. and Wang, H. (2025) A Continuous Authentication Scheme for Zero-Trust Architecture in Industrial Internet of Things. *Alexandria Engineering Journal*, **122**, 555-563. https://doi.org/10.1016/j.aej.2025.03.012

[11] Lv, F., Wang, H., Pan, Z., Sun, R., Si, S., Zhang, W., *et al.* (2025) Asynchronous Federated Learning Based Zero Trust Architecture for the Next Generation Industrial Control Systems. *Computer Networks*, **269**, Article 111459. https://doi.org/10.1016/j.comnet.2025.111459

[12] Zanasi, C., Russo, S. and Colajanni, M. (2024) Flexible Zero Trust Architecture for the Cybersecurity of Industrial IoT Infrastructures. *Ad Hoc Networks*, **156**, Article 103414. https://doi.org/10.1016/j.adhoc.2024.103414

[13] Verma, R., Indra, G., Pandey, A.K., Das, A.K. and K, V.B. (2026) ZT-RIASE: Zero Trust-Resilient Identity Attestation for Securing Smart Industrial IoT Environment. *Scientific Reports*, **16**, Article No. 22824. https://doi.org/10.1038/s41598-026-54343-0

[14] Rushdy, A. and Thorig, I. (2025) Zero Trust Architecture: A Systematic Literature Review on Adoption, Implementation and Effectiveness. 2025 2*nd International Conference on Innovations in Engineering, Science and Technology for Sustainable Development* (*ICEST*), Malé, 1-2 October 2025, 1-9. https://doi.org/10.1109/icest65883.2025.11428620

[15] Ruambo, F.A., Zou, D., Lopes, I.O., Yuan, B., Muthanna, A., Zakarya, M., *et al.* (2026) Trust Scoring Algorithms for Zero Trust-Based Software-Defined Perimeter Architectures: A Systematic Literature Review of Advancements, Challenges, and Future Directions. *Computers and Electrical Engineering*, **132**, Article 111002. https://doi.org/10.1016/j.compeleceng.2026.111002

[16] Akhmetkaliyev, A., Ala'anzy, M.A., Almsafir, M.K. and Musleh, S. (2026) Zero Trust Architecture for Industry 5.0 and Industrial IoT: A Systematic Review, Taxonomy, and Research Roadmap. *Computer Networks*, **289**, Article 112695. https://doi.org/10.1016/j.comnet.2026.112695

[17] Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., *et al.* (2021) The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *British Medical Journal*, **372**, n71. https://doi.org/10.1136/bmj.n71

[18] Kitchenham, B., Brereton, O.P., Budgen, D., *et al.* (2009) Systematic Literature Reviews in Software Engineering—A Systematic Literature Review. *Information and Software Technology*, **51**, 7-15. https://doi.org/10.1016/j.infsof.2008.09.009

[19] Feng, X. and Hu, S. (2023) Cyber-Physical Zero Trust Architecture for Industrial Cyber-Physical Systems. *IEEE Transactions on Industrial Cyber-Physical Systems*, **1**, 394-405. https://doi.org/10.1109/ticps.2023.3333850

[20] Baig, A.F., Eskeland, S. and Yang, B. (2023) Privacy-Preserving Continuous Authentication Using Behavioral Biometrics. *International Journal of Information Security*, **22**, 1833-1847. https://doi.org/10.1007/s10207-023-00721-y

[21] Abba, S.S., Obioha-Val, O.A., Ejiofor, V.O., Olaniyi, O.M. and Mayeke, N.R. (2025) Behavioral Biometrics-Powered Continuous Authentication for Zero-Trust Remote Work Environments: A Multi-Factor Identity Verification Framework. *Asian Journal of Research in Computer Science*, **18**, 20-41. https://doi.org/10.9734/ajrcos/2025/v18i12788

[22] Meng, L., Huang, D., An, J., Zhou, X. and Lin, F. (2022) A Continuous Authentication Protocol without Trust Authority for Zero Trust Architecture. *China Communications*, **19**, 198-213. https://doi.org/10.23919/jcc.2022.08.015

[23] Salman, M. and Budiyanto, A. (2026) Enhancing Industrial Cybersecurity via IoT Device-Trusted Remote Attestation Framework with Zero Trust Architecture in Brewery Operations. *Indonesian Journal of Electrical Engineering and Computer Science*, **41**, Article 720. https://doi.org/10.11591/ijeecs.v41.i2.pp720-730

[24] Jayakrishnan, S., Jain, K., Krishnan, P., N., H.N. and N, S.S. (2026). Zero Trust Architecture for MQTT-Based IoT Networks Using ESIM and IoT Safe. 2026 5*th International Conference on Computer Networks, Big Data and IoT* (*ICCBI*), Dubai, 18-20 June 2026, 464-471. https://doi.org/10.1109/iccbi68589.2026.11619769

[25] Wang, H., Yi, L., Li, J., Wang, Z., Sun, Y. and Liu, M. (2026) ZT-eSIM: A Zero Trust Continuous Authentication Framework for 5G/6G Network Access Security. 2026 7*th Information Communication Technologies Conference* (*ICTC*), Nanjing, 8-10 May 2026, 455-459. https://doi.org/10.1109/ictc70246.2026.11650271

[26] Lv, Z., Yuan, Q., Wang, X., Chen, C., Lan, J. and Wang, K. (2025) Robust Device Authentication against Environmental Interference in Fieldbus Network. 2025 8*th*

International Conference on Information Communication and Signal Processing (*ICICSP*), Xi'an, 19-21 September 2025, 741-746. https://doi.org/10.1109/icicsp66564.2025.11338345

[27] Ghnaimat, T.M., Sabri, K.E. and Obeid, N. (2026) Context-Aware Temporal Defeasible Logic Framework for Risk-Based Access Control in Zero Trust Architecture. *IEEE Access*, **14**, 128689-128709. https://doi.org/10.1109/access.2026.3724630

[28] Saha, R., Kumar, G., Conti, M., Devgun, T. and Rodrigues, J.J.P.C. (2024) AALMOND: Decentralized Adaptive Access Control of Multiparty Data Sharing in Industrial Networks. *IEEE Internet of Things Journal*, **11**, 26104-26117. https://doi.org/10.1109/jiot.2024.3392933

[29] Feng, L., Lin, J., Qiu, F., Yu, B., JIn, Z., Wang, J., *et al.* (2024) SDAC-BBPP: A Secure Dynamic Access Control Scheme with Blockchain-Based Privacy Protection for IIoT. *IEEE Transactions on Network and Service Management*, **21**, 3179-3193. https://doi.org/10.1109/tnsm.2024.3371521

[30] Murugadoss, R., Z, A.W., S, A. and R, A.B. (2026) Securing the Internet of Things: A Byzantine-Resilient Approach to Mitigating Real-Time Cyber Attacks. 2026 2*nd International Conference on Intelligent Systems and Computational Networks* (*ICISCN*), Bidar, 24-25 April 2026, 1-6. https://doi.org/10.1109/iciscn67954.2026.11566672

[31] Han, M.L., Li, J., Hu, K., Cen, Y., Jia, L. and Zhang, Z. (2025) Research and Application of Remote Operation and Maintenance Technology for Substation Monitoring System Based on Zero Trust Mechanism. 2025 2*nd International Conference on Smart Grid and Artificial Intelligence* (*SGAI*), Changsha, 21-23 March 2025, 1112-1117. https://doi.org/10.1109/sgai64825.2025.11009982

[32] Mamun, Q. and Picone, M. (2026) Zero-Trust Secure Network Slicing for Autonomous Vehicle Platooning. 2026 *IEEE International Conference on Smart Computing Workshops and Other Affiliated Events* (*SmartComp Companion*), Messina, 22-25 June 2026, 358-363. https://doi.org/10.1109/smartcomp-companion70724.2026.00077

[33] Kabwama, C.A., Businge, P., Malingu, C.J., *et al.* (2025) Graph Attention Networks for Credit Card Fraud Detection: A Relational Learning Approach. *World Journal of Advanced Research and Reviews*, **26**, 2580-2585. https://doi.org/10.30574/wjarr.2025.26.3.2400

[34] Businge, P., Agaba, I.A., Atuhaire, J.I., Nayebale, F.I., Ariho, J.G., Mugalu, B., *et al.* (2025) Adaptive Financial Fraud Detection Using Graph Neural Networks and Reinforcement Learning. *World Journal of Advanced Research and Reviews*, **28**, 842-847. https://doi.org/10.30574/wjarr.2025.28.2.3761

[35] Malingu, C.J., Kabwama, C.A., Businge, P., *et al.* (2025) Application of LLMS to Fraud Detection. *World Journal of Advanced Research and Reviews*, **26**, 178-183. https://doi.org/10.30574/wjarr.2025.26.2.1586

[36] Rguig, B. and Housni, K. (2026) A Granular Zero-Trust Cog-GAT Strategy in IoT: A Cognitive Behavioral IPS Graph Attention Mechanism for Pre-Emptive Risk Mitigation. 2026 6*th International Conference on Innovative Research in Applied Science, Engineering and Technology* (*IRASET*), FEZ, 14-15 May 2026, 1-6. https://doi.org/10.1109/iraset68627.2026.11538511

[37] Hassan, A., Rauf, A., Shafqat, N., Latif, R. and Khan, H. (2025) ZenGuard a Machine Learning Based Zero Trust Framework for Context Aware Threat Mitigation Using SIEM SOAR and UEBA. *Scientific Reports*, **15**, Article No. 35871. https://doi.org/10.1038/s41598-025-20998-4

[38] Kumar, G.H., Shelke, N., Pimpalkar, A., Saini, D.K.J.B., N, P.S. and Kumar, Y.D. (2025) Zero Trust-Enabled Digital Twins for Real-Time Anomaly Detection in Industrial Cyber Physical Systems. 2025 *Third International Conference on Networks, Multimedia and Information Technology* (*NMITCON*), Bengaluru, 1-2 August 2025, 1-6. https://doi.org/10.1109/nmitcon65824.2025.11188236

[39] Lu, J., Chang, Z., Yang, G., Zhang, H. and Zhang, H. (2026) A Zero Trust Defense Model for Hydropower Monitoring Systems to Mitigate Lateral Movement from BAS. *Data and Metadata*, **5**, Article 1448. https://doi.org/10.56294/dm20261448

[40] Zanasi, C., Magnanini, F., Russo, S. and Colajanni, M. (2022) A Zero Trust Approach for the Cybersecurity of Industrial Control Systems. 2022 *IEEE* 21*st International Symposium on Network Computing and Applications* (*NCA*), Boston, 14-16 December 2022, 1-7. https://doi.org/10.1109/nca57778.2022.10013559

[41] Lei, W.X., Pang, Z.B., Wen, H., Hou, W. and Zhang, X. (2023) Edge-Enabled Zero Trust Architecture for ICPS with Spatial and Temporal Granularity. 2023 *IEEE* 6*th International Conference on Industrial Cyber-Physical Systems* (*ICPS*), Wuhan, 8-11 May 2023, 1-6. https://doi.org/10.1109/icps58381.2023.10127999

[42] Vasilică, B., Anton, F.D., Mocanu, S. and Chiriac, B.N. (2025) Implementation and Evaluation of a Zero-Trust Security Model in Distributed Industrial Networks. 2025 25*th International Conference on Control Systems and Computer Science* (*CSCS*), Bucharest, 27-30 May 2025, 243-250. https://doi.org/10.1109/cscs66924.2025.00044

[43] Al Balushi, G.A.A. and Al Harthy, K. (2026) Integrating AI with Zero Trust for Secure Oil & Gas IoT Environments. 2026 *International Conference on Sustainable Engineering and Digital Innovation* (*ICSEDI*), Muscat, 10-12 February 2026, 1-8. https://doi.org/10.1109/icsedi66420.2026.11568399

[44] Poduvu, S., Neupane, R.L., Morel, A.E., *et al.* (2024) Task-Based Access Control for Computation and Communication in the Tactical Warfighting Edge. 2024 *IEEE Military Communications Conference* (*MILCOM*), Washington D.C., 28 October-1 November 2024, 839-846. https://doi.org/10.1109/milcom61039.2024.10773844

[45] Alshehri, A., Tufekci, B. and Tunc, C. (2024) Identification Management for Zero Trust through Network Analysis. 2024 *IEEE/ACS* 21*st International Conference on Computer Systems and Applications* (*AICCSA*), Sousse, 22-26 October 2024, 1-6. https://doi.org/10.1109/aiccsa63423.2024.10912537

[46] Ge, Y. and Zhu, Q. (2024) GAZETA: GAme-Theoretic ZEro-Trust Authentication for Defense against Lateral Movement in 5G IoT Networks. *IEEE Transactions on Information Forensics and Security*, **19**, 540-554. https://doi.org/10.1109/tifs.2023.3326975

[47] Zhang, M., Cheng, Y., Wang, H. and Lv, F. (2025) OMATE-ZT: Optimized Multi-Attribute Trust Evaluation Model for Zero-Trust in Industrial Internet of Things. 2025 *IEEE International Conference on Systems, Man, and Cybernetics* (*SMC*), Vienna, 5-8 October 2025, 5088-5094. https://doi.org/10.1109/smc58881.2025.11343034

[48] Qu, X., Ou, W., Pang, M., Chen, Y., Wu, Y., Yue, Q., *et al.* (2026) A Lightweight Zero-Trust-Based Authentication Framework for UAV Systems. *Sensors*, **26**, Article 4161. https://doi.org/10.3390/s26134161

[49] Ramzi Rashid, A., Ali, Z.L. and Al-Doori, A.S.B. (2026) Zero-Trust Architecture for Securing IoT Edge Networks against Advanced Persistent Threats. *Al-Noor Journal of Engineering Management and Computer Science*, **2**, 140-160. https://doi.org/10.71229/7ja6js06

[50] Olugbade, A., Adediji, E., Eni, F., Titilayo, D.H., Kabwama, C.A. and Agbesi, J.S.

(2025) Hybrid Quantum Machine Learning for Anomaly Detection in Critical Infrastructure Sensor Networks. *Global Journal of Engineering and Technology Advances*, **23**, 333-361. https://doi.org/10.30574/gjeta.2025.23.3.0198

[51] Al-Sadi, D. and Rjoub, A. (2025) Federated Edge AI for Adaptive Zero-Trust Security in Resource-Constrained IoT Networks. 2025 *IEEE International Smart Cities Conference* (*ISC*2), Patras, 6-9 October 2025, 1-6. https://doi.org/10.1109/isc266238.2025.11293319

[52] Pinyi, E.O., Kabwama, C.A., Zeyeum, J.N., Oluwabukola, H.P. and Ikwuogu, O.F. (2025) Federated IAM for Critical Systems: A Blockchain-Based Decentralized Identity Framework Enhanced by Federated Learning for Cross-Sector CNI Trust. *International Journal of Computer Applications Technology and Research*, **14**, 28-45. https://doi.org/10.7753/ijcatr1409.1005

[53] Hossain, A.A. and Ahner, D. (2025) Game Theory-Driven AI for Zero Trust Security. 2025 2*nd International Conference on Artificial Intelligence, Metaverse, and Cybersecurity* (*ICAMAC*), Dubai, 17-18 October 2025, 1-6. https://doi.org/10.1109/icamac67779.2025.11398547

[54] Kabwama, C.A., Ayozie, O.M., Zeyeum, J.N., Awe, A.O., Ikwuogu, O.F. and Titilayo, D.H. (2025) Generative Adversarial Network (GAN) Modeling for CNI Vulnerability Discovery: An Immutable Knowledge Base for Automated Infrastructure Hardening via Distributed Ledger Technology. *Global Journal of Engineering and Technology Advances*, **25**, 292-307. https://doi.org/10.30574/gjeta.2025.25.1.0309

[55] Malingu, C.J., Titilayo, D.H., Eni, F., Kabwama, C.A. and Anyah, V. (2024) Adversarial Machine Learning in Finance: Developing Resilient AI Models to Counter Fraudster Evasion Attacks on US Bank Security Systems. *International Journal of Computer Applications Technology and Research*, **13**, 111-137.

[56] Kabwama, C.A., Pinyi, E.O., Adediji, E., Zeyeum, J.N. and Ikwuogu, O.F. (2025) Decentralized AI-Driven Zero-Trust Architecture: Leveraging Blockchain for Immutable Policy Enforcement and Autonomous Anomaly Response in Critical Infrastructure Systems. *World Journal of Advanced Engineering Technology and Sciences*, **17**, 559-573. https://doi.org/10.30574/wjaets.2025.17.1.1427

[57] Yu, W. and Zhang, L. (2022) Research on Zero Trust Access Control Model and Formalization Based on Rail Transit Data Platform. 2022 *IEEE* 10*th International Conference on Information, Communication and Networks* (*ICICN*), Zhangye, 23-24 August 2022, 689-695. https://doi.org/10.1109/icicn56848.2022.10006520

[58] Mohseni Ejiyeh, A. (2023) Real-Time Lightweight Cloud-Based Access Control for Wearable IoT Devices: A Zero Trust Protocol. *Proceedings of the* 1*st International Workshop on Security and Privacy of Sensing Systems*, Istanbul, 12-17 November 2023, 22-29. https://doi.org/10.1145/3628356.3630118

[59] Stanojevic, M., Capko, D., Lendak, I., Stoja, S. and Jelacic, B. (2023) Fighting Insider Threats, with Zero-Trust in Microservice-Based, Smart Grid OT Systems. *Acta Polytechnica Hungarica*, **20**, 229-248. https://doi.org/10.12700/aph.20.6.2023.6.13

[60] Zhang, K., Zheng, J., Fu, J., Zhang, Y. and Ji, W. (2023) Research and Application of Zero Trust Based Secure Access to the Power Internet of Things. 2023 *IEEE* 7*th Information Technology and Mechatronics Engineering Conference* (*ITOEC*), Chongqing, 15-17 September 2023, 2356-23690. https://doi.org/10.1109/itoec57671.2023.10291965

[61] Jamil, M., Farhan, M., Ullah, F. and Srivastava, G. (2024) A Lightweight Zero Trust Framework for Secure 5G VANET Vehicular Communication. *IEEE Wireless Communications*, **31**, 136-141. https://doi.org/10.1109/mwc.015.2300418

[62] Kuang, X., Cao, Y., Hong, C., Zhang, Y., Jiang, Y. and Su, Y. (2024) Access of Power IoT Devices Based on Zero-Trust Technology. 2024 6*th International Academic Exchange Conference on Science and Technology Innovation* (*IAECST*), Guangzhou, 6-8 December 2024, 1394-1397. https://doi.org/10.1109/iaecst64597.2024.11118006

[63] Yoon, M., Seo, J., Lee, J. and Cho, K. (2024) Design and Implementation of a 5G Security Testbed Based on Zero Trust Architecture. 2024 15*th International Conference on Information and Communication Technology Convergence* (*ICTC*), Jeju Island, 16-18 October 2024, 2190-2192. https://doi.org/10.1109/ictc62082.2024.10826685

[64] Al-Balasmeh, H. (2025) Zero Trust Architecture for IoT Device Ecosystems. *International Journal of Basic and Applied Sciences*, **14**, 818-825. https://doi.org/10.14419/r30vpf59

[65] Apurva and Vetrithangam, D. (2025) Blockchain-Integrated Zero-Trust Architectures for Cybersecurity in IoT Ecosystems. 2025 *IEEE* 6*th Global Conference for Advancement in Technology* (*GCAT*), Bangalore, 24-26 October 2025, 1-6. https://doi.org/10.1109/gcat66372.2025.11368384

[66] Aydeger, A., Zeydan, E., Mangues-Bafalluy, J., Hewa, T. and Liyanage, M. (2025) A Novel Architecture with Blockchain-Based Identity Management for Industrial Systems. 2025 *IEEE Latin-American Conference on Communications* (*LATINCOM*), Antigua, 5-7 November 2025, 1-6. https://doi.org/10.1109/latincom67778.2025.11345420

[67] Cao, X., Chen, Z., Yang, M., Wang, X. and Wu, X. (2025) Zero Trust-Based Dynamic and Continuous Access Control for Mobile Devices. 2025 *IEEE* 24*th International Conference on Trust, Security and Privacy in Computing and Communications* (*TrustCom*), Guiyang, 14-17 November 2025, 2904-2910. https://doi.org/10.1109/trustcom66490.2025.00344

[68] Ibrahim, H., Ahakonye, L.A.C., Lee, J.M. and Kim, D. (2025) Synergistic Blockchain and Zero Trust Framework for Securing Industrial IoT against Cyber Threats. 2025 16*th International Conference on Information and Communication Technology Convergence* (*ICTC*), Jeju, 14-17 October 2025, 1854-1858. https://doi.org/10.1109/ictc66702.2025.11388337

[69] Kumar, L., Bais, K.S.S. and Lata, S. (2025) Securing Industrial IoT with Zero Trust: A Framework for Critical Infrastructure. 2025 *International Conference on Information, Implementation, and Innovation in Technology* (*I2ITCON*), Pune, 4-5 July 2025, 1-5. https://doi.org/10.1109/i2itcon65200.2025.11210610

[70] Ma, Z., Wei, H., Jiang, J., Wang, B., Wang, H. and Di, Z. (2025) A Lightweight Zero-Trust Authentication Architecture for IoT via Unified Enhanced FAST-SM9 and Dynamic Re-Authentication. *PLOS ONE*, **20**, e0332943. https://doi.org/10.1371/journal.pone.0332943

[71] Nair, R.R. (2025) National Resilience through Enterprise Security: The Role of Zero Trust in Protecting AI-Driven Critical Infrastructure in the United States. *Journal of International Crisis and Risk Communication Research*, **8**, 297-312. https://doi.org/10.63278/jicrcr.vi.3277

[72] Pitumpe, P.A.C.M.S., Jayasinghe, J.A.A.D.K., Madushan, N.N.A., Ahamed, R.S., Sudheera, K.L.K., Halgamuge, M.N., *et al.* (2025). A Trust Score Driven Zero Trust Architecture Model for Enhanced IoT Security. 2025 10*th International Conference on Automation, Control and Robotics Engineering* (*CACRE*), Wuxi, 16-19 July 2025, 350-357. https://doi.org/10.1109/cacre66141.2025.11119616

[73] Rusdan, M. and Ramlan, I. (2025) Approach of Zero Trust Security to Improve In-

ternet of Things Infrastructure Security. *LogicLink*, **2**, 112-123. https://doi.org/10.28918/logiclink.v2i2.12634

[74] Sadik, S. and Tashrif, M.T.A. (2025) Reinforcing Zero Trust: A Blind Blockchain-Based Security Framework for Industry 5.0. *Journal of Computational Science and Applications*, **2**, 21-30. https://doi.org/10.51846/jcsa.v2i2.4793

[75] Singh, T. and Nisha, T.N. (2025) Enhancing IoT Security with Zero-Trust Architecture: A Model Leveraging Blockchain and AI Capabilities. 2025 *International Conference on Emerging Information Technology and Engineering Solutions* (*EITES*), Pune, 24-25 July 2025, 173-179. https://doi.org/10.1109/eites66543.2025.00038

[76] Tinker, N., Boone, J. and Wang, K. (2025) A Novel Orchestration Framework for Zero Trust Unmanned Vehicular Networks in ROS 2. *SAE Technical Paper Series*, Novi, 12 August 2025, 1-12. https://doi.org/10.4271/2025-01-0434

[77] Vaisla, K.T.S. and Vaisla, K.S. (2025) AI-Powered Self-Healing Networks Using Quantum Key Rotation for Zero-Trust Architectures. 2025 *IEEE International Conference on Communication Networks and Computing* (*CNC*), Sonbhadra, 29-30 December 2025, 243-251. https://doi.org/10.1109/cnc68716.2025.11484764

[78] Wang, J., Huang, N., Wang, B., Ao, R., Fu, Q. and Guo, X. (2025) ZT-IoTrust: A Quantum-Resistant Zero Trust Framework for Secure IoT Access Control. *Electronics*, **14**, Article 4469. https://doi.org/10.3390/electronics14224469

[79] Wang, K., Hong, Y., Li, Y., Yan, R. and Feng, J. (2025) A Distributed Zero-Trust Scheme for Airborne Wireless Sensor Networks Using Dynamic Identity Authentication. *Scientific Reports*, **15**, Article No. 8036. https://doi.org/10.1038/s41598-025-91957-2

[80] Wang, Q., Ren, Z. and Cao, Y. (2025) A ZKP-Based Cross-Domain Continuous Authentication Scheme for Industrial Internet of Things. *Proceedings of the* 2025 6*th International Conference on Computer Information and Big Data Applications*, Wuhan, 14-16 March 2025, 583-591. https://doi.org/10.1145/3746709.3746811

[81] Al-Hadlaa, S., Alsumayt, A. and Alshammari, M. (2026) Secure and Efficient Authentication Scheme in IOT Environments Based OT. *Qubahan Academic Journal*, **6**, 272-307. https://doi.org/10.48161/qaj.v6n1a2073

[82] Bala, Z., Aliyu, M., Kuliya, M., Muhammed, L. and Idris, I.Y. (2026) A Behavioral Analytics Framework for Machine-Learned Insider Threat Detection. *Journal of Analytical and Applied Computer Sciences*, **2**, 47-59. https://doi.org/10.67914/jaacs/rsa/2.1/47-59

[83] Hussain, H., Mishra, S. and Alshenaifi, R. (2026) Post-Quantum Cognitive Zero Trust Architecture for Healthcare IoT Devices. *PLOS ONE*, **21**, e0348600. https://doi.org/10.1371/journal.pone.0348600

[84] Jeysuriya, K., Renjith, P.N. and Sudhakaran, G. (2026) Quantum-Resilient Cross-Trust Evaluation for Zero Trust 5G Security. *Scientific Reports*, **16**, Article No. 10714. https://doi.org/10.1038/s41598-026-44119-x

[85] Kumar, A. and Sharma, A. (2026) Anomaly-Aware Dynamic Trust Thresholding for Zero Trust Architecture for Secure E-Healthcare. 2026 4*th International Conference on Secure Cyber Computing and Communications* (*ICSCCC*), Jalandhar, 29-31 May 2026, 1237-1242. https://doi.org/10.1109/icsccc69031.2026.11600078

[86] Osilonya, V.O., Ejeh, P.O. and Isizoh, A. (2026) Enhanced Centralized Medical Records Security in a Zero-Trust-Based MFA Framework Using Formal Verification of Role-Based Access Control. *Advances in Multidisciplinary & Scientific Research Journal Publication*, **14**, 31-56. https://doi.org/10.22624/aims/maths/v14n1p3

[87] Sharma, N., Tiwari, A. and Gite, H. (2026) Zero-Trust Healthcare Data Exchange Using Permissioned Blockchain. 2026 22*nd IEEE International Colloquium on Signal Processing & Its Applications* (*CSPA*), Kuala Lumpur, 1-2 May 2026, 320-325. https://doi.org/10.1109/cspa68262.2026.11517898

[88] Singh, N., Dharaskar, B., Satyanarayana, K., Pande, D.M., Katari, T. and N, S. (2026) Zero Trust Architecture for Intelligent IoT-Based Cyber-Physical Systems. 2026 *IEEE* 1*st International Conference on Intelligent Technologies for a Sustainable and Inclusive Future* (*ICITSIF*), Indore, 29-30 May 2026, 595-600. https://doi.org/10.1109/icitsif69060.2026.11608797

[89] Urvashi, A.P., Raghuvanshi, K.K. and Ahmed, J. (2026) FL-EZTF: A Privacy-Preserving Federated Deep Learning Framework with Enhanced Zero Trust for Healthcare IoT Security. *International Journal of Engineering and Manufacturing*, **16**, 324-343.

[90] Wang, Z., Guo, Y. and Guo, Y. (2026) Blockchain-Based Zero-Trust Continuous Authentication Scheme for Medical IoT. *Journal of Parallel and Distributed Computing*, **217**, Article 105333. https://doi.org/10.1016/j.jpdc.2026.105333

[91] Yuan, C., Shan, H., Chen, M. and Wang, Z. (2026) Design and Implementation of Cloud-Ground-End Collaborative Zero-Trust Security Architecture for Industrial Drones. 2026 9*th International Conference on Advanced Algorithms and Control Engineering* (*ICAACE*), Jinan, 20-22 March 2026, 657-661. https://doi.org/10.1109/icaace69793.2026.11508881

[92] Zhang, X., Mu, Z., Mu, D. and Liu, X. (2026) A Lightweight Zero-Trust Authentication and Key Agreement Scheme for the Industrial Internet of Things. *Applied Sciences*, **16**, Article 6765. https://doi.org/10.3390/app16136765

Appendix. Core Studies

Table A1 lists the 70 core studies with their coded characteristics and evidence-maturity scores. The full coded list of all 425 included studies is provided in supplementary table S2 (separate supplementary workbook).

Table A1. Characteristics and evidence-maturity appraisal of the 70 core studies, ordered by year and first author (Q1 threat model, Q2 reproducible description, Q3 validation, Q4 realistic workload, Q5 baselines and metrics, Q6 critical-infrastructure applicability; 0 to 2 each). Constraints addressed: L latency, R resource limits, A availability, S safety, P privacy, B legacy or brownfield compatibility; NR not reported. Model: Rule = rule or threshold scoring. Eval. (highest evaluation level): dataset = public or real dataset.

#	Study	Year	Context	Identity	Model	Enforcement	Eval.	Constr.	Q1	Q2	Q3	Q4	Q5	Q6	Sum	Band
1	Shah *et al.* [8]	2021	IIoT	device	Graph	revocation	formal	RL	2	2	2	1	2	2	11	High
2	Alshomrani and Li [9]	2022	IIoT	device	Graph	NR	formal	R	2	2	2	0	1	2	9	Moderate
3	Meng *et al.* [22]	2022	IIoT	device	Hybrid	privilege	formal	LR	2	2	2	1	1	2	10	High
4	Yu and Zhang [57]	2022	ICS/OT	mixed	Hybrid	privilege	formal	none	0	1	1	0	0	0	2	Limited
5	Zanasi *et al.* [40]	2022	ICS/OT	mixed	Rule	isolation	prototype	B	1	1	2	1	0	2	7	Moderate
6	Ejiyeh [58]	2023	IIoT	mixed	Graph	privilege	formal	LAPR	1	2	2	0	1	2	8	Moderate
7	Feng and Hu [19]	2023	ICS/OT	mixed	Hybrid	privilege	simulation	S	2	2	2	1	2	1	10	High
8	Lei *et al.* [41]	2023	ICS/OT	mixed	Rule	isolation	formal	LS	1	1	1	0	0	1	4	Limited
9	Stanojevic *et al.* [59]	2023	Smart grid	mixed	Rule	isolation	testbed	AB	2	1	1	1	0	2	7	Moderate
10	Zhang *et al.* [60]	2023	Smart grid	device	Hybrid	revocation	testbed	ABR	1	1	1	2	1	2	8	Moderate
11	Alshehri *et al.* [45]	2024	ICS/OT	device	ML/DL	isolation	dataset	BR	1	1	2	1	1	2	8	Moderate
12	Feng *et al.* [29]	2024	IIoT	mixed	Blockchain	privilege	formal	PR	1	2	2	1	2	1	9	Moderate
13	Ge and Zhu [46]	2024	5G/6G edge	mixed	Bayesian	step-up	formal	LA	2	2	2	1	2	1	10	High
14	Jamil *et al.* [61]	2024	5G/6G edge	device	Graph	isolation	prototype	LSR	1	1	2	1	1	2	8	Moderate
15	Kuang *et al.* [62]	2024	Smart grid	device	ML/DL	privilege	prototype	ABR	1	1	1	1	1	2	7	Moderate
16	Poduvu *et al.* [44]	2024	5G/6G edge	mixed	Rule	privilege, revocation	testbed	ARL	2	1	2	2	1	2	10	High
17	Saha *et al.* [28]	2024	IIoT	mixed	Blockchain	privilege	prototype	LPR	1	2	2	1	2	2	10	High
18	Yoon *et al.* [63]	2024	5G/6G edge	mixed	Rule	isolation	testbed	LA	0	1	1	2	0	1	5	Limited
19	Zanasi *et al.* [12]	2024	IIoT	mixed	Rule	isolation	testbed	BLA	1	2	2	2	1	2	10	High
20	Abba *et al.* [21]	2025	Healthcare	human	ML/DL	privilege	dataset	LP	2	2	2	1	2	2	11	High
21	Al-Balasmeh [64]	2025	IIoT	device	Hybrid	privilege, isolation	testbed	RL	1	1	2	2	1	2	9	Moderate
22	Al-Sadi and Rjoub [51]	2025	IIoT	device	Federated	isolation	dataset	PRL	2	1	2	1	2	2	10	High
23	Apurva and D.Vetrithangam [65]	2025	IIoT	device	Hybrid	privilege	dataset	L	0	1	2	1	2	1	7	Moderate
24	Aydeger *et al.* [66]	2025	ICS/OT	mixed	Blockchain	revocation	prototype	LA	1	1	2	1	1	2	8	Moderate

Continued

25	Cao *et al.* [67]	2025	IIoT	mixed	Hybrid	privilege	prototype	none	1	2	2	1	1	0	7	Moderate
26	Han *et al.* [31]	2025	Smart grid	human	Rule	privilege	prototype	A	2	1	2	2	1	1	9	Moderate
27	Hossain and Ahner [53]	2025	CPS	mixed	Hybrid	privilege	formal	AS	2	1	1	0	0	1	5	Limited
28	Ibrahim *et al.* [68]	2025	IIoT	device	Hybrid	privilege	dataset	LR	0	1	2	1	2	2	8	Moderate
29	Kumar *et al.* [38]	2025	ICS/OT	mixed	ML/DL	isolation	dataset	SL	1	1	2	1	2	1	8	Moderate
30	Kumar *et al.* [69]	2025	IIoT	mixed	Rule	isolation	prototype	LAB	2	1	1	1	1	2	8	Moderate
31	Lv *et al.* [11]	2025	ICS/OT	mixed	Federated	privilege	dataset	LP	1	2	2	2	2	1	10	High
32	Lv *et al.* [26]	2025	ICS/OT	device	Rule	command	testbed	BR	2	2	2	2	1	2	11	High
33	Ma *et al.* [70]	2025	IIoT	device	Graph	step-up	formal	LR	2	2	2	1	2	2	11	High
34	Nair [71]	2025	ICS/OT	mixed	Rule	isolation	prototype	BA	1	0	1	2	1	2	7	Moderate
35	Pitumpe *et al.* [72]	2025	IIoT	device	Rule	isolation	testbed	R	0	1	1	2	0	1	5	Limited
36	Rusdan and Ramlan [73]	2025	IIoT	device	ML/DL	privilege	dataset	L	0	1	2	1	1	1	6	Moderate
37	Sadik and Tashrif [74]	2025	IIoT	mixed	Hybrid	isolation	testbed	LAP	1	2	2	1	2	2	10	High
38	Singh and Nisha [75]	2025	IIoT	device	Hybrid	privilege	prototype	R	0	1	1	1	0	1	4	Limited
39	Tinker *et al.* [76]	2025	CPS	workload	ML/DL	isolation	prototype	A	1	1	1	1	0	1	5	Limited
40	Vaisla and Vaisla [77]	2025	Smart grid	device	RL	revocation	testbed	AL	2	1	2	2	2	1	10	High
41	Vasilică *et al.* [42]	2025	ICS/OT	mixed	Rule	isolation	testbed	LAR	1	1	2	2	1	2	9	Moderate
42	Wan *et al.* [10]	2025	IIoT	mixed	Graph	revocation	formal	RL	2	2	2	0	2	2	10	High
43	Wang *et al.* [78]	2025	IIoT	device	Federated	privilege	dataset	LPR	1	1	2	1	2	2	9	Moderate
44	Wang *et al.* [79]	2025	CPS	device	Hybrid	isolation	formal	ARL	2	2	2	1	1	2	10	High
45	Wang *et al.* [80]	2025	IIoT	device	Graph	revocation	formal	PR	1	2	2	0	1	2	8	Moderate
46	Zhang *et al.* [47]	2025	IIoT	mixed	ML/DL	privilege	dataset	LS	1	1	2	2	2	2	10	High
47	Al-Hadlaa *et al.* [81]	2026	ICS/OT	device	Hybrid	step-up	formal	RA	1	1	2	1	2	2	9	Moderate
48	Bala *et al.* [82]	2026	CPS	human	ML/DL	privilege	dataset	L	2	1	2	1	2	1	9	Moderate
49	Balushi and Harthy [43]	2026	ICS/OT	mixed	Hybrid	isolation	prototype	LSB	1	2	1	1	1	2	8	Moderate
50	Ghnaimat *et al.* [27]	2026	Healthcare	human	Rule	privilege	formal	S	1	2	2	0	0	1	6	Moderate
51	Hussain *et al.* [83]	2026	Healthcare	device	Hybrid	isolation	dataset	LRP	1	2	2	1	2	2	10	High
52	Jayakrishnan *et al.* [24]	2026	IIoT	device	Graph	revocation, command	prototype	RL	2	2	2	1	1	2	10	High
53	Jeysuriya *et al.* [84]	2026	5G/6G edge	mixed	Blockchain	privilege	dataset	A	2	1	2	1	2	1	9	Moderate
54	Kumar and Sharma [85]	2026	Healthcare	mixed	ML/DL	privilege	dataset	LR	0	1	2	1	1	1	6	Moderate
55	Lu *et al.* [39]	2026	ICS/OT	mixed	Hybrid	isolation	testbed	LAS	2	1	2	2	2	2	11	High
56	Mamun and Picone [32]	2026	CPS	mixed	Hybrid	privilege, isolation	formal	LSA	2	2	2	1	2	2	11	High

Continued

57	Murugadoss *et al.* [30]	2026	CPS	workload	Federated	privilege	dataset	PA	2	1	2	1	1	1	8	Moderate
58	Osilonya *et al.* [86]	2026	Healthcare	human	Rule	privilege	formal	LAP	2	1	2	0	1	2	8	Moderate
59	Qu *et al.* [48]	2026	CPS	device	Bayesian	privilege, isolation	testbed	RL	2	2	2	2	2	2	12	High
60	Ramzi Rashid *et al.* [49]	2026	IIoT	device	Federated	isolation	dataset	LRP	2	1	2	2	2	2	11	High
61	Rguig and Housni [36]	2026	IIoT	device	Graph	isolation, command	dataset	R	1	1	2	1	1	1	7	Moderate
62	Salman and Budiyanto [23]	2026	IIoT	device	Graph	isolation	testbed	LRB	1	1	2	2	2	2	10	High
63	Sharma *et al.* [87]	2026	Healthcare	mixed	Blockchain	privilege	prototype	LP	1	1	2	1	1	1	7	Moderate
64	Singh *et al.* [88]	2026	CPS	mixed	Rule	isolation	testbed	LR	0	1	1	1	1	1	5	Limited
65	Urvashi *et al.* [89]	2026	Healthcare	mixed	Federated	isolation	dataset	PLR	0	1	2	1	2	2	8	Moderate
66	Verma *et al.* [13]	2026	IIoT	device	Graph	NR	NR	RLA	2	2	2	0	1	2	9	Moderate
67	Wang *et al.* [25]	2026	5G/6G edge	device	Graph	privilege	formal	RL	2	2	2	1	1	2	10	High
68	Wang *et al.* [90]	2026	Healthcare	device	Blockchain	revocation	formal	R	1	2	2	0	1	1	7	Moderate
69	Yuan *et al.* [91]	2026	CPS	device	Rule	revocation	prototype	LAR	1	1	2	1	1	2	8	Moderate
70	Zhang *et al.* [92]	2026	IIoT	mixed	Hybrid	step-up, privilege, revocation, command	formal	RSPA	1	2	2	0	1	2	8	Moderate