International Journal of Safety and Security Engineering
Vol. 16, No. 9, September, 2026, pp. 2123-2132
Journal homepage: http://iieta.org/journals/ijsse

A Formal Policy Framework for Trust Management in Federated IoT–Cloud Systems: Scoped Propagation, Influence Isolation and Session Freshness

Zainab Mohammed Ali, Wasan Saad Ahmed, Qusay Kanaan Kadhim*, Ahmed Al-Zaidi

Department of Computer Science, University of Diyala, Baqubah 32001, Iraq

Corresponding Author Email: dr.qusay.kanaan@uodiyala.edu.iq

Copyright: ©2026 The authors. This article is published by IIETA and is licensed under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

https://doi.org/10.18280/ijsse.160915

Received: 19 July 2026
Revised: 28 August 2026
Accepted: 9 September 2026
Available online: 30 September 2026

Keywords:
federated IoT–cloud systems, formal trust model, policy algebra, scoped trust propagation, influence isolation, session freshness

ABSTRACT

Federated Internet of Things (IoT)-cloud environments are a collection of independent organizations, diverse devices and multiple cloud providers without a single trust authority. Current trust-management approaches offer reputation aggregation, distributed auditability, or anomaly detection based on learning, but the semantics of the joint propagation, compromise containment and time-bounded evidence are often implicit. A specification framework is proposed in this paper which is deployment independent and is defined by $\Sigma = \langle N, D, C, P, T, V \rangle$. A contextual score is a combination of node reputation, device posture and behavioral reliability, and a policy algebra is a definition of local authorization, scoped propagation and evidence isolation. A request is allowed under the verification rule if there is a policy derivation, the score is at a device-specific threshold and the supporting evidence is recent and related to the current session. Given explicit assumptions, rule-inversion and evidence-admissibility arguments can be used to define three model-relative properties: authorized trust propagation, trust-influence isolation and trust freshness. An assumption-dependence analysis is used to determine how the conclusions might be invalidated if policy consistency, authenticated evidence, isolation enforcement, or freshness checks are weakened. A hypothetical pharmaceutical cold-chain scenario is used to show conflict detection, boundary enforcement and replay rejection. An author-conducted descriptive mapping is provided to show how the components of the framework relate to the capabilities that are promoted by four representative approach classes, and is not an independent or systematic validation. The framework thus offers an audit trail for reasoning before deployment on trust decisions in federated IoT-cloud systems.

1. INTRODUCTION

The Internet of Things (IoT) is increasingly deployed across organizational and cloud boundaries, creating federated environments in which independently administered devices, edge platforms, and cloud services exchange data and resources [1]. Unlike a single-domain deployment, a federated IoT–cloud system has no universal trust anchor [2]. Each participating organization retains its own policies, device-management practices, risk tolerances, and regulatory obligations [3]. Therefore, a trusted node in one organization may interact with a device or service that is subject to a different and possibly incompatible trust model [4]. This heterogeneity makes trust a cross-boundary security problem rather than a local reputation score [5]. Existing centralized, reputation-based, block chain-supported, and distributed approaches provide useful operational mechanisms [6]. The three remaining questions are: how can implicit trust spread across organizations, how is the impact of a compromised participant contained, and when should a previous trust decision be overturned [7-9]. Addressing these questions requires a formal representation that separates policy semantics from any particular cloud provider, IoT protocol, or application domain.

Previous studies have identified specific aspects of trust in the IoT, access control, and protocol behavior, but they have not jointly identified the three cross-border concerns they target: limited diffusion, effect isolation, and session novelty. In a federation, a numerical score alone cannot determine which administrative boundary may consume a trust assertion a distributed ledger does not by itself define the admissibility of evidence from a compromised participant and a previously valid credential remains unsafe unless its age and session binding are checked [10, 11].

In the field of the IoT, there is a lack of integrated, deployment-independent specifications that link policy derivation, contextual assessment, scope deployment, evidence isolation, and session regency within a single attacker model [12]. Trust can be considered a representational concept within a multi-enterprise cloud IoT consortium, using a stable mathematical framework [13]. For the explicit assumptions under which the validity of the declared trust dissemination, the isolation of the breach, and the regency of the decision can be jointly established [14]. Figure 1 summarizes the principal threat categories considered in cloud-based and federated IoT environments.

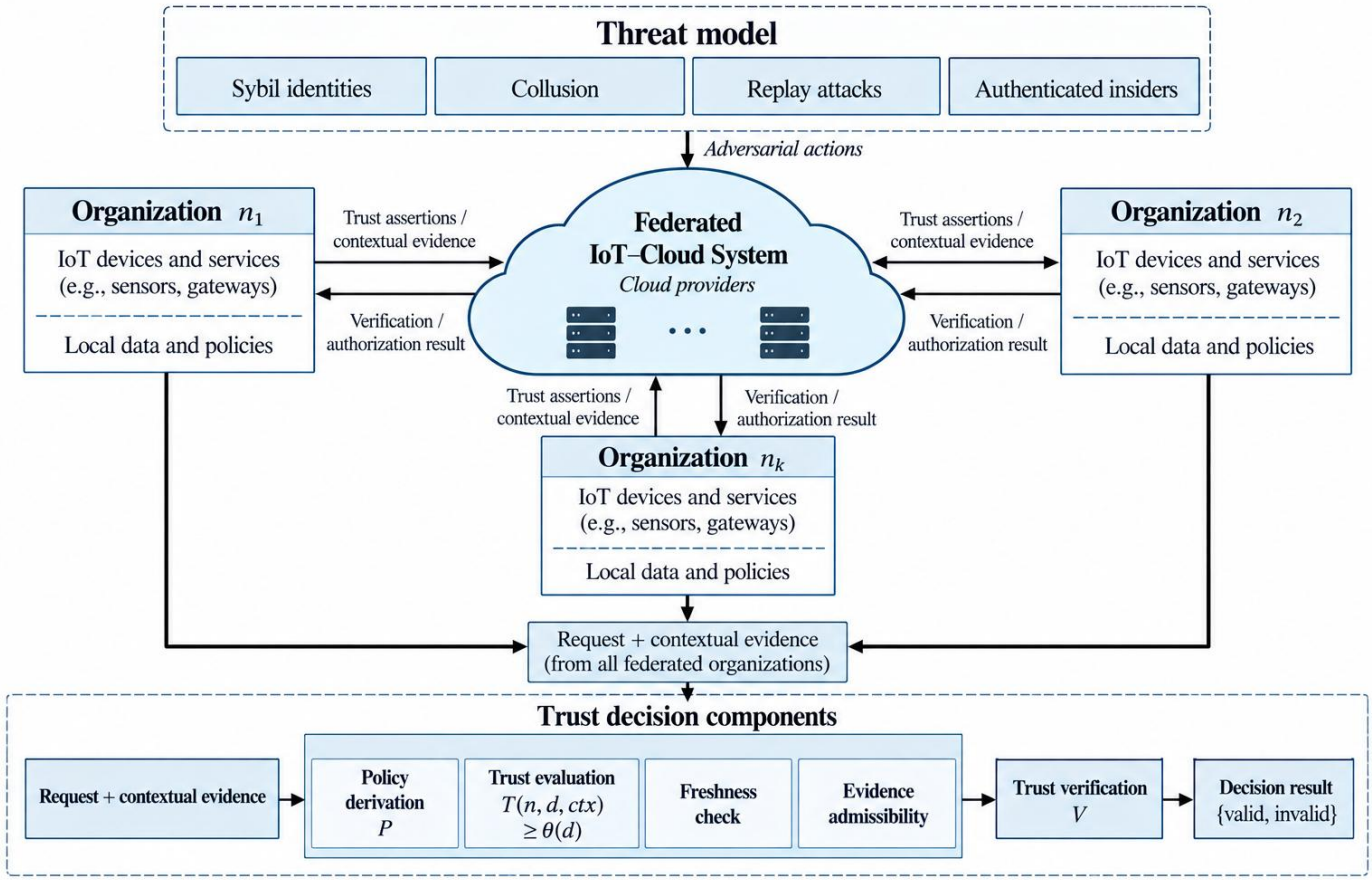


Figure 1. Threat surface in federated Internet of Things (IoT)-cloud systems

In today's interconnected digital society, communication methods have changed thanks to IoT services [15]. Vast amounts of information are available online, making it accessible anytime, anywhere [16]. From another perspective, this widespread availability of data encourages cyber attackers to exploit unknown security vulnerabilities and bypass known protection systems.

In recent years, with the increasing popularity of cloud computing, its security has become a serious problem [17]. It is better to detect and stop any attack early rather than just responding after it has occurred. Given the attacks targeting routers, cybersecurity is a concern with the rapid expansion of cloud computing [18]. According to a recent analysis by Insight, companies have seen a significant migration to the cloud computing environment, but some concerns remain, prompting other companies to review their security systems [19].

In our research, we demonstrate a trust representation framework in a multi-institutional consortium between the IoT and cloud computing using a publication-independent mathematical model. We propose explicit assumptions under which authorized trust propagation, vulnerability isolation, and session freshness can be proven. We suggest a model based on a contextual trust rating function and a uniform policy algebra, and then deduce the conditions necessary for the three properties to be realized: Scoped Propagation, Influence Isolation, and Session Freshness.

This proposal contributes to integrating and adapting established formal ideas regarding the unified cloud computing mission for the IoT. Its distinctive features are as follows:

N1—Deployment-independent system model: the tuple $\Sigma = \langle N, D, C, P, T, V \rangle$ represents the principal entities and decision components of a federated IoT–cloud environment without assuming a specific provider, protocol, or application.

N2—Contextual trust function: $T: N \times D \times Ctx \rightarrow [0,1]$ links reputation, device posture, and behavioral evidence to a device-specific verification threshold.

N3—Executable policy semantics: explicit LOCAL, PROP, ISOLATE, and DECISION rules connect policy syntax to cross-organizational authorization and evidence admissibility.

N4—Conditional property analysis: rule-inversion and admissibility arguments establish authorized propagation, influence isolation, and freshness within the stated model; the analysis does not claim unconditional security of an implementation.

N5—Structured evaluation: an illustrative cold-chain case study and a six-criterion comparison show how the framework can expose policy conflicts and assess the formal coverage of representative trust approaches.

2. RELATED WORK

The four complementary streams of work in trust management for federated IoT-cloud systems are: contextual trust evaluation, trust-aware federated learning, blockchain-supported trust management, and formal policy analysis. A review of these streams shows that there are helpful mechanisms available for estimating confidence, detecting unreliable participants, keeping track of the records, and verifying selected security properties.

The key difference for the work presented here, however, is between the production of a trust value, and the formal quantification of the locations, times, and evidence requirements for which this value can be used to make an authorization decision. Federated-learning research focuses on another aspect of the problem.

Model aggregation and unreliable contributions' impact on learning are covered by surveys of model aggregation [20] while trust-based access control and federated edge-intelligence frameworks tie participant assessment to privacy-conscious IoT operations [21]. There are related approaches to distributed threat and anomaly detection based on federated learning [22] and more general edge-AI surveys that highlight approaches to cross-device, cross-silo, and hybrid learning.

These approaches illustrate the value of trust-aware learning in operation, yet their learning pipelines do not specify policy-derivation semantics for using another organization's trust assertion or for an explicit admissibility rule that filters out tainted evidence prior to computing the trust score. In addition to trust management, blockchain also provides trust records with decentralization, traceability, integrity and auditability smart contracts has been explored in the context of formal verification in IoT access-control mechanisms [23]. These are not required to replace the proposed policy layer, but are complementary. Preserving an immutable record does not prove that the record was created along an authorized propagation path, based on admissible evidence, or met a session-freshness condition. A ledger-based implementation would then be able to maintain and account for the derivations as specified by the proposed algebra.

The closest methodological basis is formal and zero-trust research. Architecture for distributed zero-trust networks combines usage control with principles of zero-trust [24] while policy design for distributed zero-trust networks focuses on continuous, context-aware authorization [25].

The UCONABC model introduces mutable attributes and ongoing control [26] while symbolic claims and implementations and recent implementation-verification research show how symbols and protocol implementations can be mechanized [27]. The literature on these methods does not provide a scoped inter-organizational propagation method along with the boundary for evidence admissibility of compromised participants, and the boundary for freshness within a single federated trust decision rule. Hence, the research gap is not only the lack of trust scoring, distributed storage, learning-based detection, or formal verification. It is the lack of an integrated cross-organization explicit propagation, bounded influence, freshness of evidence evaluation and statement of assumptions.

The current framework responds to this more limited discrepancy by distinguishing evidence production from evidence policy derivation and by establishing the circumstances when a contextual score can assist in a federated authorization decision.

Supporting evidence indicates that there is significant variation in the types of attributes people trust, the evidence on which they base their trust, and the ways in which they assess their trust [28]. Other research works integrate device and service metrics to assess trust better [29] and extended IoT-security surveys place such tools in social, consumer and heterogeneous IoT settings [30]. The trust and reputation in IoT service composition has also been formally analyzed [31]. These studies collectively support the trust assessment but do not collectively define how a trust assertion can be authorized to cross across an organization, how evidence from a compromised participant is excluded outside of an isolation scope, and how a decision is bound to a current session.

3. FEDERATED INTERNET OF THINGS-CLOUD ARCHITECTURE

A federated IoT–cloud system connects autonomous organizations that retain control of their devices, edge infrastructure, cloud resources, and local policies [32, 33]. Trust management is complicated by three forms of heterogeneity: administrative heterogeneity, because organizations have different governance and risk tolerances; provider heterogeneity, because resources span independently managed cloud and edge platforms; and device heterogeneity, because constrained sensors coexist with gateways and higher-capacity edge nodes [34, 35]. These mixed layers of the edge and fog create their own attack surface, from device compromise to infrastructure-level threats [36]. A useful model must therefore distinguish device evidence, organizational policy, and the boundary across which a decision is consumed. The federated IoT–cloud architecture considered in this study is illustrated in Figure 2.

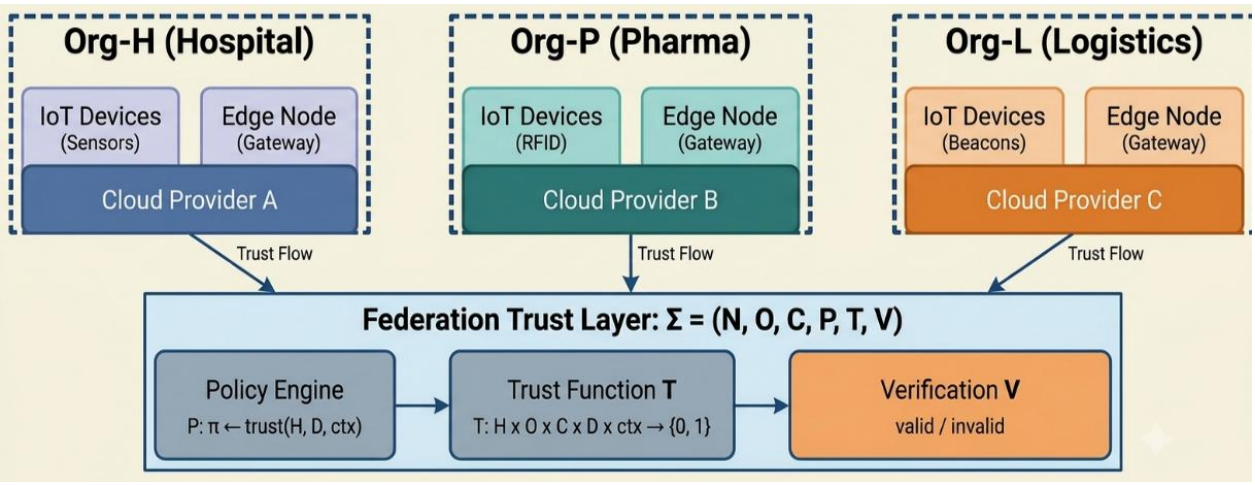


Figure 2. Federated Internet of Things (IoT)-cloud system architecture

Note: Σ = <N, D, C, P, T, V> represents the system model. Three autonomous organizations share IoT infrastructure across heterogeneous cloud providers, while trust relationships are managed through the federation trust layer.

Trust is contextual one party relies on another to perform a specified action under stated conditions [37]. Direct trust derives from first-hand observations, whereas indirect trust uses recommendations or reputation. Federated trust adds an administrative dimension: evidence or a decision produced in one organization is considered by another [38]. Such reuse must be explicitly defined and cannot be assumed to be globally transitive solely because the numerical trust score is high.

The threat model concentrates on four risks associated with federation: Sybil identities that bias recommendations, colluding participants that organize false evidence, replay of credentials that are not within their authorized time or session [39], and authenticated insiders who make false assertions. These risks highlight the importance of authenticated evidence provenance, admissibility filtering, scoped propagation, and freshness-aware verification. The symbolic model does not cover physical compromise and cryptographic implementation errors [40].

The framework draws on RBAC, ABAC, and usage-control ideas [41]. Roles may structure local policy ownership, attributes supply contextual evidence for T, and freshness supports re-evaluation when evidence or session state changes. The proposed rules operate above these mechanisms they specify whether a federated trust assertion is derivable and admissible, while an implementation may realize the attributes and enforcement using any suitable access-control technology [42].

The formal model is the Dolev-Yao symbolic abstraction, where the cryptographic primitives are perfect and an adversary is only able to control the communication channels but is not able to get a protected value without the proper key [43], Policy algebra provides a structural framework, and first-order inference rules define its meaning, resulting in transparent, handwritten derivations. Coding rules into a proof assistant, SMT parser, or protocol validator is future-proof work and is necessary before automated verification can be implemented [44].

4. METHODOLOGY

The methodology for implementing the framework sequentially begins with monitoring contextual indicators for IoT devices, including reputation (*rep*), device integrity (*pos*), and behavior (*beh*), with recording of monitoring time (t_{obs}) and session ID (*sid*). In the second stage, the overall trust function is mathematically calculated using a weighted equation, and policy algebra is applied to restrict trust transfer and isolate compromised nodes to protect the system. Finally, the results undergo a robust real-time validation mechanism that compares the value to the minimum required threshold and checks session viability to prevent time-based retransmission attacks. The process concludes with a decisive automated decision to either securely accept or outright reject the request.

Figure 3 shows the methodology representation of the trust management framework for the IoT and shared cloud computing systems (unified cloud IoT system framework), which summarizes the technical structure and implementation mechanism of the mathematical and security model across three main axes.

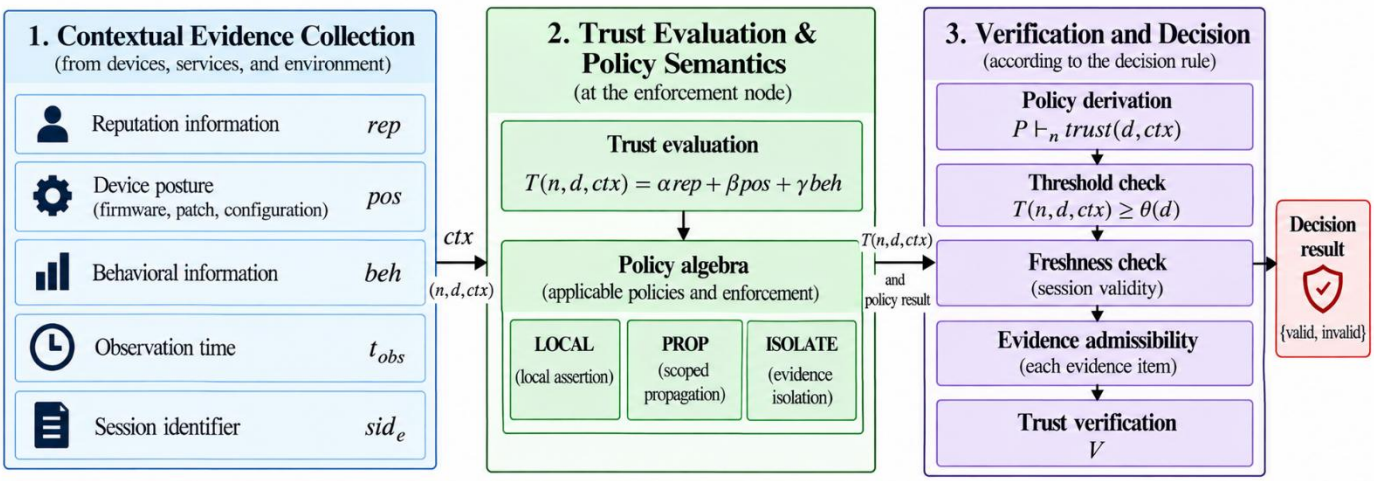


Figure 3. A framework for managing trust in Internet of Things (IoT) and cloud computing systems

4.1 System model

We model a federated IoT-Cloud system as the six-component tuple:

Definition D1 (System Model):

$\Sigma = <N, D, C, P, T, V>$

N: finite non-empty set of federated nodes (organizations)

D: finite non-empty set of IoT devices

C: finite non-empty set of cloud providers

P: finite set of trust policies over $N \times D \times Ctx$

T: trust evaluation function (Definition D3)

V: trust verification function, $V: N \times D \times Ctx \times \mathbb{R}^+ \times SID \rightarrow$ {valid, invalid} with *SID* being the set of current session identifiers.

Definition AM1 (Federated Dolev–Yao Adversary): Let $\mathcal{A}$ be a symbolic network adversary and let $K\mathcal{A}^0$ contain public identifiers, public keys, public policies, and all local state, evidence, and credentials obtained from corrupted nodes $N\mathcal{A} \subseteq N$. Its derivable knowledge is $K\mathcal{A} = \mathrm{DY}(K\mathcal{A}^0)$, the closure under message composition, decomposition, encryption, and decryption with keys already in $K\mathcal{A}$. The adversary may intercept, delay, drop, replay, reorder, and synthesize network messages; corrupt nodes in $N\mathcal{A}$; and issue assertions using acquired credentials. It cannot break cryptographic primitives, cannot derive an uncompromised secret key, cannot alter the protected policy set at an honest node, or cannot evade the

trusted verification and enforcement components assumed in A4. Authenticated provenance in A3 identifies the node to which evidence is attributable, including a corrupted origin. Thus, the model represents network control and compromised federation nodes while excluding cryptographic implementation failure, physical capture, and compromise of V or the enforcement mechanism.

Assumptions A1–A5 used by the conditional soundness result:

A1 (policy consistency): no request derives both trust and distrust at the same node.

A2 (closed decision scope): every request submitted to V has either a trust derivation or a distrust derivation; requests outside this scope are denied.

A3 (evidence integrity): every component used by T is normalized to [0,1], authenticated, provenance-bound, and admitted by the ISOLATE rule.

A4 (complete enforcement): V implements the DECISION rule and cannot bypass policy, threshold, or freshness checks.

A5 (non-degenerate parameters): $\theta(d) \in (0,1]$ and $\Delta(d) > 0$ for every $d \in D$; $\alpha, \beta, \gamma \geq 0$ and $\alpha + \beta + \gamma = 1$.

4.2 Trust evaluation function

Definition D2 (Contextual Attribute Space):

$$Ctx = (rep, pos, beh, t_{obs}, sid_e)$$

where,

rep $\in$ [0,1]: node reputation score aggregated from federation history.

pos $\in$ [0,1]: device-posture score derived from firmware, patch, and configuration evidence.

beh $\in$ [0,1]: behavioral-reliability score, where higher values indicate behavior closer to the accepted norm; $t_{obs} \in \mathbb{R}^+$ is the observation timestamp; and sid_e is the session identifier bound to the trust evidence.

Definition D3 (Trust Evaluation Function):

$$T : N \times D \times Ctx \rightarrow [0,1]$$
$$T(n,d,ctx) = \alpha \cdot rep + \beta \cdot pos + \gamma \cdot beh$$

where, $\alpha, \beta, \gamma \in [0,1]$ and $\alpha + \beta + \gamma = 1$.

Definition D4 (Freshness-Aware Trust Decision):

$$Fresh(d, ctx, t_{now}, sid_{now}) \Leftrightarrow 0 \leq t_{now} - t_{obs} \leq \Delta(d) sid_e = sid_{now}$$
$$V(n,d,ctx,t_{now},sid_{now}) = valid \Leftrightarrow T(n,d,ctx) \geq \theta(d) \wedge Fresh(d,ctx,t_{now},sid_{now})$$

where, θ: $D \rightarrow (0,1)$ is the device-specific trust threshold and Δ: $D \rightarrow \mathbb{R}^+$ is the permitted evidence age.

Definition D5 (Policy Syntax):

P can contain local (n, q, S), propagate (n_s, n_t, q, S), isolate ($\hat{n}$, B), and deny (n, q, S) for nodes n, n_s, $n_t \in N$, assertion q, and scope $S \subseteq D \times Ctx$. The predicate owner(d) refers to the node that owns device d.

Definition D6 (Judgments and Evidence Admissibility):

$P \vdash_n q(d, ctx)$ denotes that assertion q for (d, ctx) is derivable at node n. Adm(e, n, d, ctx) $\in$ {0,1} indicates whether evidence item e is admissible for that decision.

Definition D7 (LOCAL Rule):

$$local(n,q,S) \in P \wedge (d,ctx) \in S \Rightarrow P \vdash_n q(d,ctx)$$

where, *local* is only able to assert at the node specified by the local policy.

Definition D8 (PROP Rule):

$$P \vdash n_s\ q(d,ctx) propagate(n_s,n_t,q,S) \in P(d,ctx) \in S \Rightarrow P \vdash n_t\ q(d,ctx)$$

The only rule that moves an assertion from one enforcement node to another is PROP.

Definition D9 (ISOLATE Rule):

$$isolate(\hat{n}, B) \in P \wedge evidence\ e\ attributable\ to\ \hat{n}(n,d,ctx) \notin B \Rightarrow Adm(e,n,d,ctx) = 0$$

If not, admissibility is based on the authenticated-provenance and policy checks in A3.

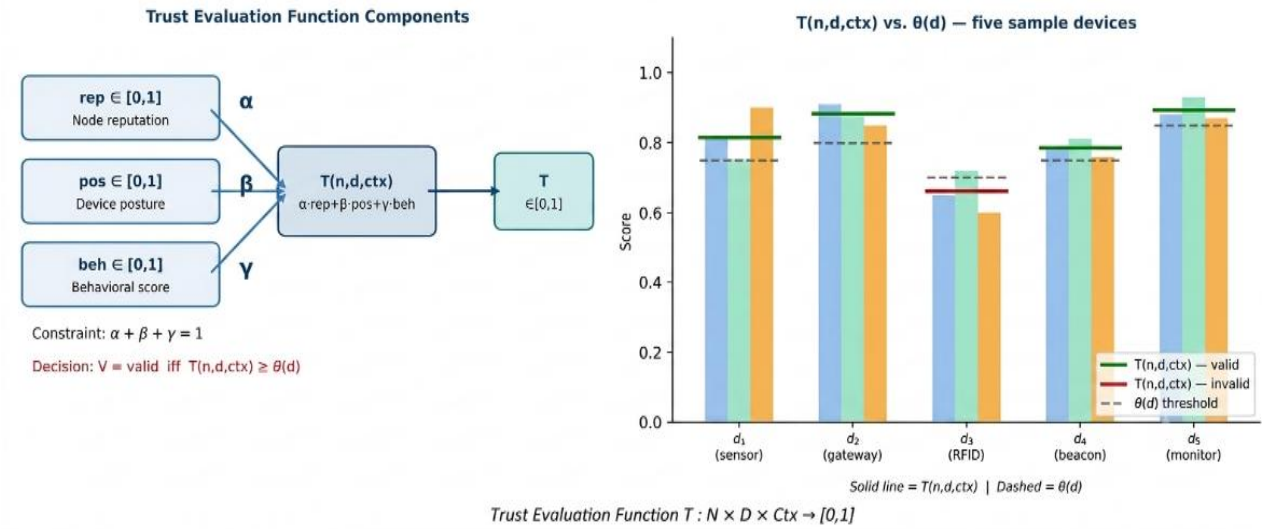


Figure 4. Trust evaluation and freshness-aware verification

Note: The weighted score combines *rep*, *pos*, and behavioral reliability; *V* grants access only when the score reaches $\theta(d)$ and the evidence satisfies Fresh

Definition D10 (DECISION Rule):

$$P \vdash_n trust(d, ctx) \wedge T(n, d, ctx) \geq \theta(d) Fresh(d, ctx, t_{now}, sid_{now}) \forall e \in E_T : Adm(e, n, d, ctx) = 1 \Rightarrow P \vdash_n accept(d, ctx, t_{now}, sid_{now})$$

where, E_T is the evidence used to compute T. If any premise is false, V returns invalid under A4.

Definition D11 (Consistency and Closed Decision Scope):

P is consistent for request r when it is not the case that both $P \vdash_n$ trust(r) and $P \vdash_n$ distrust(r). Its decision scope is closed when every request submitted to V has a trust or distrust derivation; a request outside that scope is denied. These conditions correspond to A1 and A2. Figure 4 summarizes the trust-evaluation components and the freshness-aware verification process.

4.3 Security properties and formal proofs

Lemma 1—Zero trust lower bound:

$$V(n, d, ctx, t_{now}, sid_{now}) = valid \Leftrightarrow T(n, d, ctx) \geq \theta(d) \wedge Fresh(d, ctx, t_{now}, sid_{now})$$
$$T = \alpha \cdot 0 + \beta \cdot 0 + \gamma \cdot 0 = 0$$

By A5, $\theta(d) > 0$; therefore, the threshold condition in D4 fails and V returns invalid.

Lemma 2—Decision characterization:

$$P \vdash_n accept(d, ctx, t_{now}, sid_{now}) \Leftrightarrow \text{all four DECISION premises hold}$$

Proof (⇒): inversion of the last rule in the derivation of accept exposes the four DECISION premises.

Proof (⇐): if the four premises hold, one application of DECISION derives accept.

By A4, $V(n, d, ctx, t_{now}, sid_{now})$ = valid exactly for derivable accept judgments.

Lemma 3—Session-bound freshness:

For $\sigma_1 = \langle n, d, ctx_1, t_1 \rangle$ and $\sigma_2 = \langle n, d, ctx_2, t_2 \rangle$, where ctx_1 contains sid_1 and ctx_2 contains sid_2, evidence from σ_1 is acceptable in σ_2 only if Fresh (d, ctx_1, t_2, sid_2) holds.

$$t_2 - t_{obs,1} > \Delta(d) sid_1 \neq sid_2 \Rightarrow \neg Fresh(d, ctx_1, t_2, sid_2)$$
$$V(n, d, ctx, t_{now}, sid_{now}) = valid \Leftrightarrow T(n, d, ctx) \geq \theta(d) \wedge Fresh(d, ctx, t_{now}, sid_{now})$$

A new valid decision therefore requires evidence that is both sufficiently recent and bound to the current session. □

Property 1—Authorized Trust Propagation (ATP)

Statement: if node n_t accepts a device owned by $n_s \neq n_t$ on the basis of a trust assertion originating at n_s, the derivation contains an applicable PROP rule whose scope includes (d,ctx). When explicitly authorized by a propagate policy in P.

$$P \vdash n_t accept(d, ctx, t_{now}) owner(d) = n_s \wedge n_s \neq n_t \Rightarrow \exists q, S : propagate(n_s, n_t, q, S) \in P \wedge (d, ctx) \in S$$

Thus, the property restricts propagation; it does not claim that trust is mathematically transitive.

Proof: $P \vdash n_t$ trust(n_t,d,ctx)is the result of inverting DECISION. Since the supporting assertion is created at (n_s) and is used at (n_t), LOCAL cannot model this cross-boundary step:

$$P \vdash n_s\ q(d, ctx) \not\Rightarrow \text{LOCAL}\ P \vdash n_t\ q(d, ctx)$$

By Definitions D7 and D8, PROP is the only rule that changes the enforcement node from n_s to n_t. Inverting PROP therefore yields

$$propagate(n_s, n_t, q, S) \in P$$

and

$$(d, ctx) \in S$$

Thus, the required propagation policy must be explicitly contained in P:

$$propagate(n_s, n_t, q, S) \in P$$

Corollary 1.1: In the event that there is no relevant PROP rule, a remote assertion cannot be used to derive an accept at the target node. Inter-federation trust thus needs policy authorization.

Property 2—Trust-Influence Isolation (TI)

Statement: Evidence attributable to a compromised node ($\hat{n}$) cannot influence a decision outside the boundary defined by ($isolate(\hat{n},B)$).

$$isolate(\hat{n}, B) \in P \wedge (n, d, ctx) \notin B \Rightarrow Adm(e_{\hat{n}}, n, d, ctx) = 0$$

Therefore, there can be no derivation of DECISION outside (B) that uses (e_n) in the calculation of (rep), (pos), or (beh). Evidence: ISOLATE indicates evidence that can be attributed to ($\hat{n}$) as inadmissible beyond (B).

Assumption A3 states that all the components of the score must be computed based on admissible evidence, whereas DECISION states that all the evidence items employed by (T) must be admissible. Thus, a derivation involving (e_n) not in (B) has no premise required and cannot be carried out.

Property 3 — Trust Freshness (TF)

Statement: stale evidence or evidence bound to another session cannot support an accept derivation authorize access in session $s2$ at $t2 > t1$ without re-evaluation.

$$\neg Fresh(d, ctx, t_{now}, sid_{now}) \Rightarrow P \nvdash_n accept(d, ctx, t_{now}, sid_{now}) \wedge V(n, d, ctx, t_{now}, sid_{now}) = invalid$$

Proof: DECISION contains Fresh as a mandatory premise. If the evidence age exceeds $\Delta(d)$, lies in the future, or sid differs from the current session, that premise is false. No application of DECISION is possible; A4 therefore makes V invalid. A replay is rejected when the replayed credential is stale or session-mismatched, even if its numerical score remains above $\theta(d)$.

$$V \text{ at } t' \text{ evaluates } T(n, d, ctx'), \text{where } ctx' \text{ contains } t' \neq t$$

The relationship among the three model-relative security properties and the conditional soundness result is summarized in Figure 5.

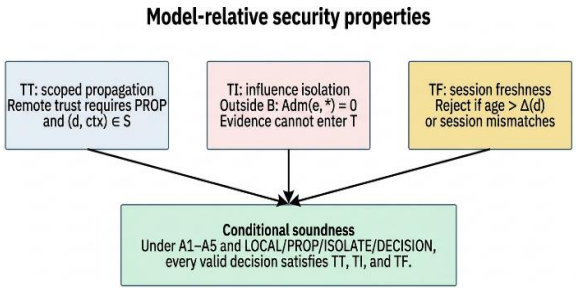


Figure 5. Three security properties and soundness theorem
Note: Left: ATP needs an explicit propagation policy. Center: TI blocks false trust at the Iso(n*) boundary. Right: TF is able to beat replay by using session non-stationarity.

5. EVALUATION

This section describes the six criteria based on the proposed definitions and conditional results, using an author's descriptive mapping. The four approach classes were chosen based on the literature cited and evaluated by the authors; there was no systematic-review protocol or independent assessors or reproducible external scoring procedure. Therefore, the mapping is not an empirical benchmark and does not constitute an independent validation of the proposed framework, but rather shows differences in formal emphasis.

(1) M1—Reputation-based IoT trust: These approaches define some trust attributes and evaluation mechanisms but do not explicitly specify all four inference rules or the three model-relative properties. Therefore, C1 and C3 are assessed as partial, while the remaining criteria are not explicit in the selected sources.

(2) M2—Blockchain-based distributed trust: Blockchain-based approaches manage trust records and provide auditability. However, policy derivation and session freshness remain separate concerns. C1 and C3 are partially addressed within the selected survey scope, whereas C2 and C4–C6 are not explicit.

(3) M3—Trust-aware federated learning: Learning-based mechanisms identify unreliable participants or support adaptive participation but do not specify the semantics of LOCAL, PROP, ISOLATE, and DECISION. Therefore, C1 and C3 are assessed as partial, while C2 and C4–C6 are not explicit in the selected works.

(4) M4 Formal and multi-criteria IoT trust: formal service-composition analysis provides stronger reasoning than heuristic scoring, but the combined federated propagation, evidence-isolation, and session-freshness specification remains outside its scope. C1, C3, and C5 are partial relative to the criteria; C2, C4, and C6 are not explicit.

The six formal-analysis criteria used in the descriptive mapping are summarized in Table 1.

Table 1. Defined formal analysis criteria

ID	Criterion	Formal Referent
C1	Formal system model defined	Definition D1
C2	Explicit formal threat model	Definition AM1
C3	Formal trust evaluation function	Definitions D3–D4
C4	Policy algebra with federated operators	Definitions D5–D11
C5	Formally proven trust properties	Properties ATP, TI, and TF
C6	Conditional soundness result and assumption-dependence analysis	Theorem 1

6. RESULTS AND DISCUSSION

The results of this study are presented through deductive analysis, an illustrative scenario, and a literature-based comparison. The evaluation does not use a prototype or experimental dataset; instead, it examines policy derivability, evidence admissibility, policy conflicts, and formal specification coverage. Therefore, it does not evaluate runtime performance, detection accuracy, or operational security.

6.1 Formal results

R1—Authorized **propagation.** If $n_s \neq n_t$, any request accepted at n_t on the basis of a trust assertion originating from n_s must be supported by an applicable $propagate(n_s, n_t, q, S)$ policy such that $(d, ctx) \in S$. If the propagation policy or scope membership is absent, the remote assertion cannot complete an accept derivation. This result establishes scoped propagation rather than unrestricted mathematical transitivity.

R2—Influence isolation. Suppose $isolate(\hat{n}, B) \in P$. Evidence attributable to the compromised node n̂ is inadmissible outside the isolation boundary B. Accordingly, such evidence cannot influence T or support a DECISION derivation for any $(n, d, ctx) \notin B$. Under A3, only admissible evidence can contribute to T, and DECISION verifies the admissibility of every evidence item used in the score. This result contains the modeled influence of a compromised participant; it does not claim that the participant or the provenance mechanism cannot itself be compromised.

R3—Session freshness. An otherwise adequate trust score is rejected when $t_{now} < t_{obs}$, $t_{now} - t_{obs} > \Delta(d)$, or the evidence session identifier is not equal to the current session identifier. Thus, a past decision cannot be reused simply because its numerical trust score is still above $\theta(d)$. The evidence needed to support a new valid decision must meet the age and session-binding requirements.

6.2 Joint conditional result

Theorem 1 is a synthesis of R1-R3 in one decision semantics. In A1-A5, all accepted requests are authorized derivations, based on evidence that has been accepted within the relevant isolation boundary, and meet the device-specific threshold, and the freshness condition. The conclusion is conditional and relative to the given model: in case a corresponding assumption is dropped, a premise on which the proof relies might also fail.

6.3 Illustrative policy analysis

The pharmaceutical cold-chain case is an example of how the framework examines the trust decisions between federated participants. A local policy grants the monitored device, a propagation policy limits the participant and context to which its trust assertion can be consumed, and an isolation policy ensures that evidence attributable to a compromised federation node does not affect requests beyond its stated boundary. Symbolic evaluation reveals a conflict when the same request elicits trust and distrust. The conflict in the case of the request under consideration can be solved by narrowing the broader policy to the exceptional context. The scenario identifies three causes of rejection that can be obscured by a single trust score: the lack of propagation authorization, the use of evidence that

is not within its isolation boundary, and the lack of freshness or session binding. The solution to one conflict under analysis does not create uniformity in all the possible requests. Automated request enumeration or machine-checked verification would be exhaustive to analyze.

6.4 Descriptive criteria mapping

The proposed specification instantiates C1–C6 by construction, since they are derived from the proposed specification. As shown in Table 2, the selected sources of reputation-based, blockchain-based, trust-aware federated-learning, and formal/multi-criteria sources highlight different subsets of these author-defined concepts. This observation is only to clarify the formal scope of the framework intended; it is not evidence of superiority over the compared approaches. The mapping does not show that the proposed framework is more secure, accurate, scalable, or efficient than the compared approaches. The present specification does not implement those approaches, which offer complementary operational capabilities, such as reputation aggregation, learning-based detection, and tamper-evident storage. The authors' interpretive basis is made visible in Table 2. Partial means that a related concept exists, but it is not expressed in the specific form that the author-defined criterion is expressed; Not explicit means that the criterion is not expressed in that form in the selected sources. These labels are descriptive judgments based on the stated rubric and on the literature selected and are not scores that are assessed independently.

The most important lesson is that trust scoring and authorization are used to solve different issues. (T) is a measure of contextual confidence, and policy derivation is whether that confidence can be utilized by a particular node in a given device and context. Both must ensure that a high trust score does not silently cross federation boundaries.

The three properties are mutually dependent. Scoped propagation constrains the use of a trust assertion; influence constrains what evidence can be used to influence a score once a participant has been compromised; and freshness constrains the time and session in which the resulting decision can be used. These properties, when combined in DECISION, give a clear foundation on which to accept or reject and the assumptions made in each decision. D10-D11 are used to define policy inconsistency and incomplete scope of decision to be audited. The exemplary conflict shows how symbolic derivation can show overlapping allow and deny results. Automated auditing would involve encoding the policy algebra and inference rules in an SMT solver, model checker, proof assistant, or specialized policy-analysis tool.

The values of α, β and γ are deployment-specific and satisfy ($\alpha + \beta + \gamma = 1$). The framework does not specify an empirically optimal assignment; calibration, sensitivity analysis, and threshold selection remain deployment activities. Similarly, the adversary bound alone does not demonstrate resistance to Sybil and collusion attacks. TI also depends on authenticated provenance, protected isolation policies, and trustworthy enforcement.

The analysis has four main limitations. First, the proofs are handwritten rather than machine-checked. Second, the case study is hypothetical and does not measure latency, throughput, scalability, or attack-detection accuracy. Third, the framework assumes the integrity of the policy-decision and enforcement components and does not model their compromise. Fourth, it does not address cryptographic-protocol correctness, physical capture, supply-chain security, incident response, or vulnerability management.

Table 2. Descriptive mapping of defined criteria across representative federated Internet of Things (IoT) trust approaches

Criterion	M1 Reputation	M2 Blockchain	M3 Trust-Aware FL	M4 Formal/Multi
C1—System model	Partial	Partial	Partial	Partial
C2—Threat model	Not explicit	Not explicit	Not explicit	Not explicit
C3—Trust function	Partial	Partial	Partial	Partial
C4—Policy algebra	Not explicit	Not explicit	Not explicit	Not explicit
C5—Proven properties	Not explicit	Not explicit	Not explicit	Partial
C6—Conditional soundness analysis	Not explicit	Not explicit	Not explicit	Not explicit

7. CONCLUSIONS

In this study, a deployment-independent formal policy framework for trust management in federated IoT–cloud systems were introduced. The six-component model $\Sigma = \langle N, D, C, P, T, V \rangle$ connects the contextual scoring with explicit local authorization, propagation of evidence within scope of an organization, isolation of evidence, threshold evaluation and freshness of evidence in a session. The rule-inversion and evidence-admissibility arguments are used to build three model-relative properties that are joint: authorized trust propagation, trust-influence isolation, and trust freshness. The illustrative cold-chain analysis demonstrates the ability of the policy algebra to differentiate between policy conflicts, boundary violations, stale or session-mismatched evidence. The descriptive literature mapping provides an explanation of the proposed specification in relation to the capabilities that are highlighted in four representative approach classes but is not an independent and systematic validation.

Since no implementation or operational deployment was evaluated, these results measure only formal specification coverage and internal derivability; they do not demonstrate superior empirical security, accuracy, efficiency, or scalability. Therefore, the framework is best viewed as an auditable basis for pre-deployment reasoning and future machine-checked implementation.

Future work will encode the definitions, inference rules, and conditional theorem in a proof assistant, SMT solver, or model checker to automatically evaluate policy consistency, decision-scope completeness, and counterexamples. A reference implementation should also integrate the policy layer with an IoT–cloud testbed to evaluate decision latency, throughput, scalability, enforcement overhead, and resilience under replay, Sybil, collusion, and compromised-node scenarios.

Additional empirical studies are needed to calibrate α, β, γ, $\theta(d)$, and $\Delta(d)$ with representative device and organizational risk profiles; perform sensitivity and ablation studies; and explore dynamic, distributed, and partially trusted policy engines. Generalizing the model to compromised PE/PEP

components, governance-conscious coalition threats, cryptographic-protocol information, and actual multi-organization policy sets would help understand which guarantees hold outside of the present assumptions.

REFERENCES

[1] Riehle, D.M., Arz von Straussenburg, A.F., Blazevic, M. (2026). Edge AI in the social internet of things: A systematic review of trends and research needs. Management Review Quarterly, 1-34. https://doi.org/10.1007/s11301-026-00588-y

[2] Zhang, Y., Li, C., Liu, L., Sun, Y., Xu, X. (2026). Federated-trust sharded blockchain for real-time forensics and secure data collaboration in cooperative V2X. Journal of King Saud University Computer and Information Sciences, 38: 382. https://doi.org/10.1007/s44443-026-00813-4

[3] Kadhim, Q.K., Ahmed, S.T., Kadum, J., Turki, E.M., Kadhim, A.K. (2026). Detecting identity theft attacks in cloud security based on artificial intelligence techniques. In Proceedings of the International Conference on Applied Innovations in IT, pp. 1093-1099. https://doi.org/10.25673/123682

[4] Kumara, S. (2025). Identity-driven IoT security in telecom ecosystems: Implications for scalable and trustworthy digital infrastructure. International Journal of Applied Mathematics, 38(12s): 2797-2816. https://doi.org/10.12732/ijam.v38i12s.1588

[5] Dockara, T.R., Malhotra, M. (2026). TrustDS: Policy-compiled governance and verifiable evidence for cross-cloud marketplace analytics under explicit security assumptions. Scientific Reports, 16: 17958. https://doi.org/10.1038/s41598-026-48740-8

[6] More, J.S., Lokare, R., Bodade, V.V. (2025). Edge-assisted privacy-preserving data aggregation in vehicular ad hoc networks. International Journal of Advanced Science and Engineering, 12(2): 5738-5752. https://doi.org/10.29294/IJASE.12.2.2025.5738-5752

[7] Sarfaraz, A., Chakrabortty, R.K., Essam, D.L. (2023). The implications of blockchain-coordinated information sharing within a supply chain: A simulation study. Blockchain: Research and Applications, 4(1): 100110. https://doi.org/10.1016/j.bcra.2022.100110

[8] Cao, N., Sun, B., Li, W., Yue, G. (2025). The implicit theories of trust: The more individuals believe trust to be unchangeable, the more they tend to trust others. BMC Psychology, 13: 950. https://doi.org/10.1186/s40359-025-03267-x

[9] Murtezaj, D., Rössert, L.J., Abdelrahman, Y., Paneva, V., Alt, F. (2026). Small talk, big impact: The role of everyday conversations in cybersecurity practices. In Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems, pp. 1-26. https://doi.org/10.1145/3772318.3791412

[10] Shi, Y. (2025). Risk prevention in global cross-border data flows: Challenges and China's strategic responses. International Journal of Digital Law and Governance, 2(2): 373-399. https://doi.org/10.1515/ijdlg-2025-0013

[11] Sifakis, N. (2026). Global virtual prosumer framework for secure cross-border energy transactions using IoT, multi-agent intelligence, and blockchain smart contracts. Information, 17(4): 396. https://doi.org/10.3390/info17040396

[12] Liang, S., Qiao, Z., Bai, T., He, Y., Chen, D.E., Fu, S. (2026). A system-level framework for evaluating privacy in hybrid LLM deployments. Algorithms, 19(6): 500. https://doi.org/10.3390/a19060500

[13] Ren, Y., Wang, Z., Sharma, P.K., Alqahtani, F., Tolba, A., Wang, J. (2025). Zero trust networks: Evolution and application from concept to practice. Computers, Materials & Continua, 82(2): 1593-1613. https://doi.org/10.32604/cmc.2025.059170

[14] Alshaikh, M., Mehmood, S., Amin, R., Alsubaei, F.S. (2025). The impact of cybersecurity through knowledge sharing practices: Limitations, analysis of current trends and future research directions. International Journal of Advanced Computer Science & Applications, 16(3): 1007-1029. https://doi.org/10.14569/IJACSA.2025.0160398

[15] Chithaluru, P., Jyothi, B.V., Alharithi, F.S., et al. (2026). A scalable and secure federated learning authentication scheme for IoT. Scientific Reports, 16: 7888. https://doi.org/10.1038/s41598-026-37541-8

[16] Fereidouni, H., Fadeitcheva, O., Zalai, M. (2025). IoT and man-in-the-middle attacks. Security and Privacy, 8(2): e70016. https://doi.org/10.1002/spy2.70016

[17] Ali, T., Al-Khalidi, M., Al-Zaidi, R. (2026). Information security risk assessment methods in cloud computing: Comprehensive review. Journal of Computer Information Systems, 66(1): 123-150. https://doi.org/10.1080/08874417.2024.2329985

[18] Shah, A.S., Karabulut, M.A., Kamruzzaman, A., Alharthi, D., Bradford, P.G. (2025). A survey on artificial intelligence and blockchain clustering for enhanced security in 6G wireless networks. Computers, Materials & Continua, 84(2): 1981-2013. https://doi.org/10.32604/cmc.2025.064028

[19] Celiktas, B., Birgin, B., Tok, M.S. (2025). An analysis of enterprise-level cloud transition barriers within the technology-organization-environment (TOE) framework and strategic solution proposals. Bilişim Teknolojileri Dergisi, 18(4): 335-354. https://doi.org/10.17671/gazibtd.1678237

[20] Qi, P., Chiaro, D., Guzzo, A., Ianni, M., Fortino, G., Piccialli, F. (2024). Model aggregation techniques in federated learning: A comprehensive survey. Future Generation Computer Systems, 150: 272-293. https://doi.org/10.1016/j.future.2023.09.008

[21] Padmavathi, V., Saminathan, R. (2025). A federated edge intelligence framework with trust based access control for secure and privacy preserving IoT systems. Scientific Reports, 15: 35832. https://doi.org/10.1038/s41598-025-19712-1

[22] Rahmati, M., Pagano, A. (2025). Federated learning-driven cybersecurity framework for IoT networks with privacy preserving and real-time threat detection capabilities. Informatics, 12(3): 62. https://doi.org/10.3390/informatics12030062

[23] Guo, Z. (2025). Blockchain-enhanced smart contracts for formal verification of IoT access control mechanisms. Alexandria Engineering Journal, 118: 315-324. https://doi.org/10.1016/j.aej.2024.12.109

[24] Ameer, S., Praharaj, L., Sandhu, R., Bhatt, S., Gupta, M. (2024). ZTA-IoT: A novel architecture for zero-trust in IoT systems and an ensuing usage control model. ACM Transactions on Privacy and Security, 27(3): 1-36.

https://doi.org/10.1145/3671147
[25] Sandjaja, F.R., Majeed, A.A., Abdullah, A., Wickremasinghe, G., Rafferty, K., Sharma, V. (2025). Policy design in zero-trust distributed networks: Challenges and solutions. arXiv preprint arXiv:2508.04526. https://doi.org/10.48550/arXiv.2508.04526
[26] Park, J., Sandhu, R. (2004). The UCONABC usage control model. ACM Transactions on Information and System Security, 7(1): 128-174. https://doi.org/10.1145/984334.984339
[27] Bhargavan, K., Hansen, L.L., Kiefer, F., Schneider-Bensch, J., Spitters, B. (2025). Formal security and functional verification of cryptographic protocol implementations in rust. In Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25), Taipei, Taiwan, pp. 2729-2743. https://doi.org/10.1145/3719027.3765213
[28] Ferraris, D., Fernandez-Gago, C., Roman, R., Lopez, J. (2024). A survey on IoT trust model frameworks. The Journal of Supercomputing, 80(6): 8259-8296. https://doi.org/10.1007/s11227-023-05765-4
[29] Alghofaili, Y., Rassam, M.A. (2022). A trust management model for IoT devices and services based on the multi-criteria decision-making approach and deep long short-term memory technique. Sensors, 22(2): 634. https://doi.org/10.3390/s22020634
[30] Patil, D.A., G, S. (2025). A comprehensive survey on securing the social internet of things: Protocols, threat mitigation, technological integrations, tools, and performance metrics. Scientific Reports, 15: 40190. https://doi.org/10.1038/s41598-025-23865-4
[31] Ahmed, A.I.A., Hamid, S.H.A., Gani, A., Abdelaziz, A., Abaker, M. (2023). Formal analysis of trust and reputation for service composition in IoT. Sensors, 23(6): 3192. https://doi.org/10.3390/s23063192
[32] Kadhim, Q.K., Yusof, R., Mahdi, H.S., Selamat, S.R. (2017). The effectiveness of random early detection in data center transmission control protocol-based cloud computing networks. International Journal on Communications Antenna and Propagation, 7(5): 357-363. https://doi.org/10.15866/irecap.v7i5.10104
[33] Alsultani, H.S.M., Kanaan, Q., Khudhair, I.Y. (2018). Empirical investigation of TCP incast congestion in wireless cloud computing networks. Journal of Computer Science, 14(5): 663-672. https://doi.org/10.3844/jcssp.2018.663.672
[34] Sefati, S.S., Arasteh, B., Halunga, S., Fratu, O. (2025). A comprehensive survey of cybersecurity techniques based on quality of service (QoS) on the Internet of Things (IoT). Cluster Computing, 28(12): 792. https://doi.org/10.1007/s10586-025-05449-z
[35] Kabier, M.K., Abduljabbar, Z.A., Hussain, M.A., et al. (2026). Comprehensive security review and challenges for smart and power grids to prevent cyber-attacks in IoTs. MethodsX, 17: 104043. https://doi.org/10.1016/j.mex.2026.104043
[36] Kadhim, Q.K., Altameemi, A.I., Abdulkader, R.M., Ahmed, S.T. (2024). Enhancement of data center transmission control protocol performance in network cloud environments. Ingenierie des Systemes d'Information, 29(3): 1115-1123. https://doi.org/10.18280/isi.290329
[37] Klingbeil, A., Grützner, C., Schreck, P. (2024). Trust and reliance on AI—An experimental study on the extent and costs of overreliance on AI. Computers in Human Behavior, 160: 108352. https://doi.org/10.1016/j.chb.2024.108352
[38] Fotia, L., Delicato, F., Fortino, G. (2023). Trust in edge-based internet of things architectures: State of the art and research challenges. ACM Computing Surveys, 55(9): 1-34. https://doi.org/10.1145/3558779
[39] Hadi, T.H., Kadum, J., Kadhim, Q.K., Ahmed, S.T. (2024). An enhanced cloud storage auditing approach using Boneh-Lynn-Shacham's signature and automatic blocker protocol. Ingénierie des Systèmes d'Information, 29(1): 261-268. https://doi.org/10.18280/isi.290126
[40] Abdullah, A.J., Hameed, M.R., Kadhim, Q.K., Ahmed, S.T., Kadhim, A.K. (2025). An interpretable hybrid framework for principal component analysis-extreme gradient boosting and a single-class support vector machine for zero-day penetration detection. International Journal of Safety and Security Engineering, 15(12): 2551-2559. https://doi.org/10.18280/ijsse.151212
[41] Chen, J., Schinke, L., Gong, X., Hoppen, M., Roßmann, J. (2024). Interoperable access and usage control of self-sovereign digital twins using ODRL and I4.0 language. In Proceedings of the 9th International Conference on Internet of Things, Big Data and Security (IoTBDS 2024), pp. 75-85. https://doi.org/10.5220/0012686500003705
[42] Nazir, A., Rehmani, M.H., Butler, B., O'Shea, D. (2026). Access control in healthcare IoT: A comprehensive survey. Engineering Reports, 8(4): e70766. https://doi.org/10.1002/eng2.70766
[43] Dolev, D., Yao, A. (1983). On the security of public key protocols. IEEE Transactions on Information Theory, 29(2): 198-208. https://doi.org/10.1109/TIT.1983.1056650
[44] Ahman, D., Bhargavan, K., Bond, B., et al. (2026). Project everest: Perspectives from developing industrial-grade high-assurance software. ACM Transactions on Programming Languages and Systems, 48(2): 1-64. https://doi.org/10.1145/3805702