frontiers | Frontiers in Computer Science

TYPE Review
PUBLISHED 29 October 2025
DOI 10.3389/fcomp.2025.1670473

OPEN ACCESS

EDITED BY
Andrejs Romanovs,
Riga Technical University, Latvia

REVIEWED BY
Larry C. Bates,
Independent Researcher, Detroit, United States
Abdul Muhammed Rasheed,
Noorul Islam University, India

*CORRESPONDENCE
Suresh Sankaranarayanan
ssuresh@kfu.edu.sa

RECEIVED 21 July 2025
ACCEPTED 14 October 2025
PUBLISHED 29 October 2025

CITATION
Shujaa W, Alanzi M and Sankaranarayanan S (2025) Enhancing IoT security through blockchain integration. *Front. Comput. Sci.* 7:1670473. doi: 10.3389/fcomp.2025.1670473

Enhancing IoT security through blockchain integration

Wafa Shujaa, Mona Alanzi and Suresh Sankaranarayanan*

Department of Computer Science, College of Computer Science and Information Technology, King Faisal University, Al Ahsa, Saudi Arabia

Blockchain technology has emerged as a potential solution for securing the rapidly expanding Internet of Things (IoT). This review critically analyzes 49 recent scientific publications to assess the current state of blockchain-based IoT security. We examine the strengths and weaknesses of various approaches, focusing on their ability to address data integrity, authentication, and access control vulnerabilities. The review identifies persistent challenges related to scalability, energy efficiency, and privacy, and proposes actionable future research directions. These directions include the development of context-aware security protocols, adaptive trust models, and privacy-preserving analytics techniques. This paper provides a valuable resource for researchers seeking to advance the field of blockchain-based IoT security.

KEYWORDS

blockchain, Internet of Things, IoT, security, privacy

1 Introduction

The IoT's (Internet of Things) fast growth has revealed the lack of device identity, key management, data integrity, and access control that has existed for a long time in heterogeneous, resource-constrained nodes (Obaidat et al., 2024). Essentially, this proliferation is characterized by billions of energy-sensitive, connected devices that pose privacy and security issues because of single points of failure, opaque data governance, and excessive trust in third parties that act as intermediaries (Alzoubi et al., 2022).

In addition to the resource constraints, the cryptographic overheads for securing endpoints greatly limit the scalability of networks that handle real-time telemetry at scale (Abang et al., 2024). Blockchain can deliver clear logs, witness changes in state, and offer programmable controls via smart contracts when it is implemented sensibly and as part of a bigger security framework (Barazanchi and Hashim, 2023). Anyway, decentralisation, rather than "eliminating" central authorities, can still keep the number of middlemen low in specific workflows and under clearly defined scenarios (Obaidat et al., 2024).

One of the current developments in the field of blockchain technology is the energy-conscious consensus system (for instance PoS/DPoS) which is capable of relieving some of the blockchain network's energy consumption problems (Barazanchi and Hashim, 2023). Furthermore, the use of layered architectures in blockchain networks enables such networks to distribute and thus prevent bottlenecking in the process of load in the actual work (Eghmazi et al., 2024b). However, the overall performance of these models is calculated based on a combination of their implementation in realistic environments where latency, throughput, and integration constraints are considered (Abang et al., 2024). So, we cite the evidence of experiments and prototypes versus implementation in production deployments, quite strictly, and we avoid extending the benefits beyond the tested areas (Obaidat et al., 2024). As a step to go beyond mere descriptions, we have brought the identity and trust-chain lifecycle (enrolment → credential issuance → authentication → authorisation → transaction logging → revocation/rotation → audit) to the forefront and depicted which on-chain versus off-chain control.

This review synthesizes findings from recent (2020–2025) studies to:

(1) Recognize major privacy and security issues of IoT that the adoption of a blockchain could relieve the IoT stated manner (Obaidat et al., 2024).
(2) Work out a systematic classification for the IoT solutions that use blockchain technology (BIoT) on the basis of architecture, consensus, application domain, and security objective (Shammar et al., 2021).
(3) Integrate the strengths and trade-offs (e.g., auditability vs. latency; privacy strength vs. device budgets; portability vs. domain fit) through a brief benchmarking rubric (security/performance/resource/governance/interoperability) to support a data-driven appraisal process (Abang et al., 2024).
(4) And uncover the issues (e.g., identity lifecycle governance, benchmarking, real-world validation) and suggest feasible research directions that resonate with the regulatory and operational conditions (Obaidat et al., 2024).

We generally adopt a critical stance: Is it really that blockchain has the capacity to help meet certain security goals, especially those of auditability, non-repudiation, and tamper-evident logging, that is if the context, architecture, and operational maturity are the right ones (Tranvåg, 2025). Moreover, security measures such should device identity proofing, hardware-backed key custody, and secure firmware pipelines that are necessary and not replaced by on-chain mechanisms remain.

2 Literature review

The relevant literature was systematically identified through keyword searches in major scholarly databases (IEEE Xplore, SpringerLink, ScienceDirect, and arXiv), following a topic-centred screening protocol (Obaidat et al., 2024). Search terms included combinations of "IoT security," "blockchain integration," "privacy," "consensus algorithm," "smart contracts," and "trust management," reflecting the core technical axes of BIoT research (Obaidat et al., 2024). To ensure relevance, the search focused on peer-reviewed articles published between 2020 and 2025 that explicitly investigate blockchain-based security or privacy for IoT (Obaidat et al., 2024). The selected articles were then categorised along four axes to enable structured comparison (Shammar et al., 2021).

(1) Blockchain Architecture. We distinguish permissioned designs (e.g., Hyperledger Fabric), permissionless implementations (e.g., Ethereum-based), and layered/hybrid models that partition responsibilities across tiers (Eghmazi et al., 2024a).
(2) Consensus Algorithm. We group studies by mechanism—PoW/PoS, PBFT-style finality, and lightweight or reputation-based approaches tailored to constrained devices (Yuan et al., 2025).
(3) Application Area. We assign research to domains such as healthcare, smart home/city, industrial IoT, and supply-chain. For example, in smart-home settings, a consortium-chain message-authentication scheme anchors signed telemetry to curb spoofing (Liu et al., 2023); and in healthcare, an opportunistic access-control model combines blockchain with ML-based context checks to improve auditability and traceability (Anjum et al., 2025).
(4) Security Objective. We classify works by primary goal—authentication/access control, integrity, privacy preservation, or trust management, aligning with established taxonomies in recent reviews (Shammar et al., 2021).

Across domains, BIoT integration has been explored chiefly in pilots and prototypes rather than production deployments, and reported gains are often domain-specific with limited portability under different workloads or threat models (Obaidat et al., 2024). To ground terminology and avoid over-generalisation, subsection 2.5 formalises the identity and trust-chain lifecycle and makes explicit which controls are anchored on-chain versus which remain off-chain (e.g., device attestation, secure boot, and hardware-backed key custody) (Lorych and Plappert, 2024).

The Figure 1 illustrates how blockchain could be applied, under stated assumptions, to support decentralized identity, data integrity, and device trust, with on-chain anchors (e.g., revocation, audit hashes) and off-chain mandatory controls (device attestation, secure boot, key custody).

2.1 Blockchain architecture

Many studies have delved into designing architectural frameworks that would effectively combine blockchain with IoT for achieving scalability, decentralization, and safe data management; nevertheless, the overall benefit is dependent on the context and is limited by device budgets, integration overheads, and governance realities (Obaidat et al., 2024; Abang et al., 2024; Eghmazi et al., 2024b). In reality, on-chain components are required to be compatible with off-chain controls (device attestation, key custody, secure boot), which, most often, are the ones that set the end-to-end risk.

A study introduces a lightweight, permissioned-blockchain group-key protocol for clustered devices that significantly reduces control-plane overhead (Maeng et al., 2022). Still, the paper only provides limited information about the system's performance under dynamic, large-scale, and heterogeneous networks, thereby, adaptability, failure modes, and revocation latency remain unaddressed (Abang et al., 2024; Mazzocca et al., 2024a).

One more idea for IIoT data flows to be transparent is the proposal of a decentralised architecture with real-time blockchain layers to eliminate the need for a central broker (Latif et al., 2020). The auditability can be raised; however, as the network gets larger, so does the computational complexity and message amplification, which puts a limit on the number of resource-limited nodes and gateways that can be adopted (Abang et al., 2024; Yuan et al., 2025).

To partition responsibilities, one such as hierarchical design introduces multi-tier blockchains, which not only enhance capacity but also the extent of the admin control (Oktian et al., 2020). Although, specialised bridges are essential to allow communication between different protocols due to the diversity of the protocols, this in turn results in interoperability and lifecycle management across vendors being more complex (Eghmazi et al., 2024b; Obaidat et al., 2024).

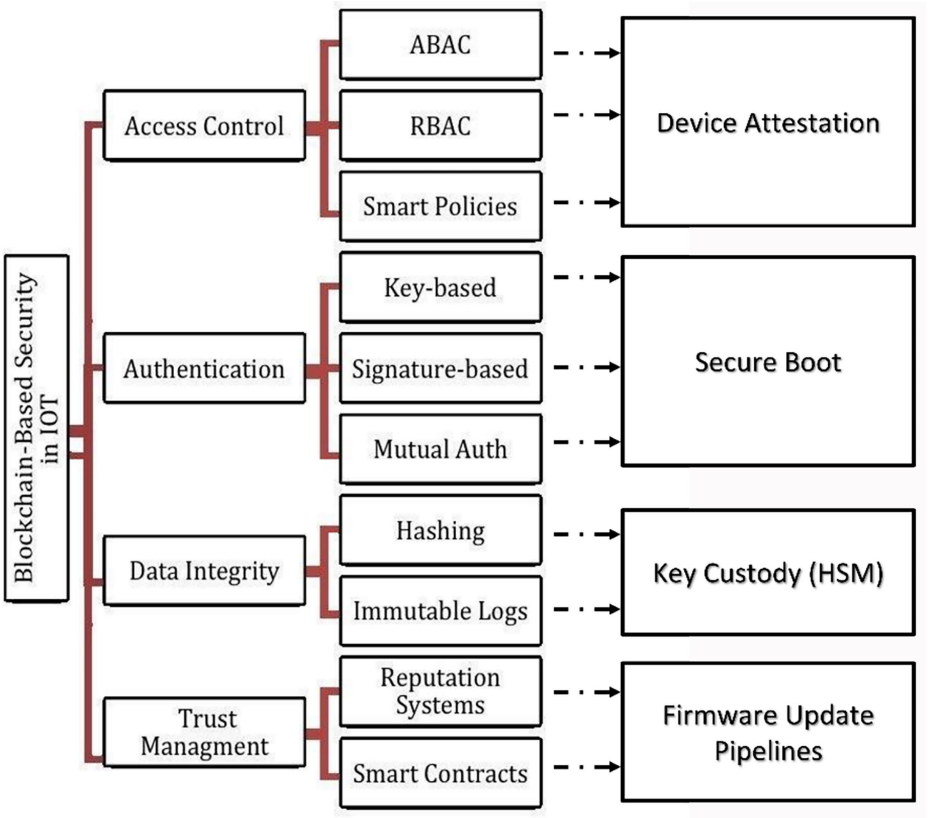

FIGURE 1
Blockchain-based security in IoT.

By implementing such a four-layer stack, streaming can be made scalable, where the private blockchain is integrated with a Kafka-based pipeline (Eghmazi et al., 2024a). The project is a good demonstration of practicable scalability and privacy partitioning, but the issues of complexity in the daily operations and the high price of the setup - in particular multi-tenant, multi-vendor deployments with uneven SRE capacity still remain (Eghmazi et al., 2024b; Abang et al., 2024).

These architectures reveal the same conflicts multiple times: throughput/latency and energy efficiency whence auditability and policy transparency are demanded. After all, most of the evaluations are pilots/prototypes rather than production deployments, so generalisability and field validation are still at the initial stage (Obaidat et al., 2024; Eghmazi et al., 2024b; Lorych and Plappert, 2024). As a result, we consider blockchain as a supplement to off-chain identity and firmware-security controls rather than the solution that entirely replaces them, and these trade-offs are reflected in our comparative analysis (Section 3) and the identity and trust-chain lifecycle (Section 2.5).

2.2 Consensus mechanism

Consensus design is the main point through which blockchain and IoT are integrated, however, the benefit of such a system is still dependent on the context of a non-hardware or low-latency environment. The envelope of security/performance depends on the complexity of the messages, hypotheses of synchrony, the number of members in the committee/the rate of replacement, and the resistance against Sybil attacks—all of which are overlapping with energy budgets and wireless variability (Abang et al., 2024; Yuan et al., 2025; Kim and Kim, 2024).

One of the methods in the field of high-volume transactions with anonymity incites the use of group signatures with batch verification as a way to increase processing effectiveness (Basudan, 2023). Nevertheless, the model here still presupposes quite stable connectivity—made worse with the re-transmissions and re-batching under lossy links that can diminish p95/p99 latency and predictability (Abang et al., 2024; Kim and Kim, 2024). The privacy–performance trade-off is still a matter to be regulated in heterogeneous nodes. The hybrid framework for mobile/vehicular IoT is a combination of the PBFT model and the support for anonymous and dynamic participation (Vangala et al., 2022). However, it should be kept in mind that the compute/communication costs are raised by quadratic messaging and view-change overheads and as a result, strict real-time operation on lightweight nodes without gateway offload or smaller committees is faced with a big challenge (Yuan et al., 2025; Banupriya and Sharmila, 2024).

For constrained devices, a lightweight protocol demonstrates high throughput and low latency in simulation (Natraj et al., 2025); at industrial scale and partial synchrony, leader contention/timeouts can re-introduce bottlenecks, requiring parameter tuning (committee sizing, timeout policy) and adversarial failure-mode testing (Abang et al., 2024; Yuan et al., 2025). To trim communication, a reputation-based mechanism adapts consensus roles to node trust levels (Zhao

et al., 2024). This improves scalability/energy use but opens attack surface (reputation poisoning/collusion) unless backed by robust admission control and periodic re-randomisation (Obaidat et al., 2024; Yuan et al., 2025).

In an effort to reduce energy consumption, a PoS + BFT-inspired model is proposing to keep finality, but at the same time power down the system (Barazanchi and Hashim, 2023). Nevertheless, the range of security covered by staking concentration, partitions, and adaptive adversaries is minimally accounted for—formal verification and experiments under adverse conditions are needed (Yuan et al., 2025; Abang et al., 2024).

The lower message complexity and faster finality that can be emulated by latency/energy improvements are, however, a trade-off in resilience to churn, partitions, and Byzantine behavior; as a matter of fact, safety margins conversely being stronger result in higher communication/compute overhead (Yuan et al., 2025; Banupriya and Sharmila, 2024; Abang et al., 2024). To enable rigorous cross-study comparison (Section 3), we choose the Benchmarking Rubric encompassing security (safety/liveness under churn/faults), performance (p95 latency, burst throughput), resource (energy/tx, RAM/flash), governance (revocation propagation, committee-rotation latency), and interoperability (gateway failure modes) as our metric. Wherever consensus-critical telemetry is logged, on-chain attestations should be used, whereas heavy cryptography and device attestation, even if telemetry is off-chain, can be considered (See Section 2.5).

2.3 Security goals

The literature addresses the fundamental goals of security—authentication, access control, integrity, and privacy—however, the overall benefit to network security is frequently dependent on the context of device budgets, latency restrictions, and identity-lifecycle management gaps (Obaidat et al., 2024). Moreover, the implementation of more robust privacy measures and more detailed policy models generally leads to higher computing, storage, and key management overhead for the nodes with limited resources (Hu, 2023).

For lightweight authentication, a recent paper presents a protocol adjusted to the most limited resource budgets that decreases the per-handshake cost and accelerates the establishment of trust (Yang et al., 2021). The account of the behavior of the system under heterogeneous links and large traffic bursts is very limited, thus scalability is still regarded as an open question (Abang et al., 2024). Besides, the latency of revocation and credential-rotation are also barely outlined (Mazzocca et al., 2024a). To link integrity with secrecy, another work branch suggests contract-mediated validation with zero-knowledge proofs (Kaur and Ali, 2021). The step of ZK proof generation and verification, which is the main cause of the processing overhead and latency, and hence the challenge for real-time IIoT control loops, is discussed in (Ramezan and Meamari, 2024b).

The survey, which is comprehensive at the threat-landscape level, outlines risks of the blockchain–IoT integration and gives a preview of mitigations (Singh et al., 2021). As a result, a lot of the security measures proposed are still at the concept stage with very few implementations that can withstand the insider threat and the cleverness of the adaptive attackers (Obaidat et al., 2024).

Recently, changes in the firmware and data flow have signaled the advent of privacy-preserving improvements, where ZK-based protection is offered to ensure the secrecy of the data and provide the evidence of the absence of tampering in the decentralized sirmetting (Ramezan and Meamari, 2024a). Their large computational and memory footprint make it very difficult to deploy them on low-powered edge devices (Ramezan and Meamari, 2024b). Another stream fuses CP-ABE with blockchain to boost fine-grained authorisation, that is a measure for better accountability as well as non-repudiation (Lee et al., 2023). Besides that, encryption overhead along with key lifecycle complexity are two major operational factors (Hu, 2023). The usability of such systems can be further impacted in mobile or dynamic topologies (Yang et al., 2024). A lightweight scheme for efficient mutual authentication exploits modular square-root cryptography to reduce resource usage to a minimum (Yang et al., 2021). However, to be really secure, the assurance of long-term cryptography and the tightness of parameters will need more work that is beyond the scope of near-term performance (Obaidat et al., 2024).

Three tensions keep coming back throughout the work: more strong personal details versus the device budget, richer policies against latency and operational complexity, and lightweight primitives versus long-term confidence (Obaidat et al., 2024). Audit hashes and revocation events as on-chain anchors can raise easier verification levels (Tranvåg, 2025). Off-chain controls, for example, device attestation, secure boot, and key custody, are always there and indispensable for end-to-end assurance (Lorych and Plappert, 2024). To do a thorough cross-study comparison, we use the benchmarking rubric with latency and burst throughput as performance baselines to set performance metrics (Abang et al., 2024). The means of governance are judged through revocation-propagation latency (Mazzocca et al., 2024a). Interoperability is gauged through the examination of gateway failure modes and portability factors (Obaidat et al., 2024).

2.4 Application domain

Across different sectors, there has been wide interest in exploring the integration of blockchain with IoT. These sectors have diverse security, scalability, and privacy needs. But most of the evidence supporting such an integration is based on pilots/prototypes rather than the actual deployment of the production, and the reported improvements are usually limited to a specific domain with little portability under different workloads and threat models (Obaidat et al., 2024). For example, in smart-home environments, signed telemetry is at the core of data integrity and dynamic audit functionalities, which are enabled by a consortium-chain message-authentication system (Liu et al., 2023). The device-key management for the lifecycle of the device has to be very accurate in the real-world scenario, and high-frequency traffic can cause audit delays and verifier load, thereby affecting the system's responsiveness (Abang et al., 2024). Medical field-wise, a blockchain system is usage for an opportunistic access-control model. The model is composed of machine learning-based context signals and aims to provide access in the real-time situation, which is very important during an emergency, situations (Anjum et al., 2025). Besides that, ML integration complicates the tuning/monitoring process and can lead to a change in bottleneck location to feature quality and model drift, as per the authors' disclosure (Obaidat et al., 2024).

In IIoT, a trust-scoring and secure-transmission model employs distributed ledger to figure out the trustworthiness of a device and guard telemetry (Rathee et al., 2022); still, the dependence on coordinator nodes can cause the same problems that the decentralisation goals try to overcome, i.e., bottlenecks and single points of failure (Abang et al., 2024). A domain solution for access control and device identity is designed to prevent the abuse of devices such as crypto-mining on compromised ones (Janani and Ramamoorthy, 2023); however, the technology remains only partially capable of confronting adaptive threats and new hardware platforms if there were no ongoing policy/firmware updates (Lorych and Plappert, 2024). For city/industrial applications, the authors implemented a four-layer stack that a private blockchain with stringent access control to manage dynamic data volumes (Eghmazi et al., 2024a). The necessary infrastructure and the amount of integration work needed are significantly large, this in turn limits the possible usage in resource-limited settings and smaller deployments (Eghmazi et al., 2024b).

The three themes that are common to all areas recurred in their respective domains: (i) the governance of the identity lifecycle is the key to the provision of sustained assurance (Mazzocca et al., 2024a); (ii) the throughput/latency limitations are frequently noticed at the gateways and coordinators rather than the on-chain (Abang et al., 2024); and (iii) the portability gets worse when the domain-specific assumptions have already leaked into the core architecture (Obaidat et al., 2024). So, we explicitly identify those things that are on-chain, for instance, audit hashes and revocation events (Tranvåg, 2025), and those things are off-chain, device attestation, secure boot, and key custody (Lorych and Plappert, 2024). The Benchmarking Rubric (Section 3) with latency and burst throughput (performance), energy/tx and RAM/flash (resources), policy-enforcement correctness and MTTR (security), revocation propagation (governance), and gateway failure modes (interoperability) is our recommended method for the future evaluation of domain solutions. We are also able to use this setting to guard against the common mistake of over-generalizing the results of domain-bound studies to wider deployments (Obaidat et al., 2024) (see Table 1).

2.5 Identity and trust-chain lifecycle in BIoT

Whether the network of connected devices (BIoT—Blockchain IoT) is successful or not, one of the main factors is the identity governance system, which must be robust enough to manage different types of devices with limited resources (Mazzocca et al., 2024a). We envision the lifecycle of the system from start to finish as: enrollment → credential issuance → authentication → authorization → transaction logging → revocation/rotation → audit. Although blockchain can act as a revocation event anchor, notarise key-state changes, and offer tamper-evident logs (Tranvåg, 2025), it seems that private-key custody, device attestation, and secure boot are operations that remain off-chain and rely on hardware roots of trust and operational runbooks (Lorych and Plappert, 2024).

2.5.1 Enrollment and issuance

It is advisable that devices be enrolled through certified supply-chain/operator procedures (El-Hajj and Beune, 2024). Credentials which may be public keys, certificates, or verifiable credentials also have validity periods, recovery methods, and revocation endpoints (Mazzocca et al., 2024b). On-chain anchoring logs the issuance metadata and hash commitments whereas the secrets are not allowed to be changed or updated in device/HSM boundaries (Tranvåg, 2025). Hardware-backed trust (TPM/TEE) is the basis for the safe provisioning and upgrade routes (Lorych and Plappert, 2024).

2.5.2 Authentication and authorization

Authentication is a combination of device-held keys and nonce/timestamp challenges which makes it difficult for replay (Obaidat et al., 2024). Authorisation policies can be present in smart contracts or in off-chain PDP/PEP engines, while on-chain attestations can keep records of grants/denials for auditability (Obaidat et al., 2024). Attribute-centric or context-aware models (e.g., CP-ABE) may enhance the accuracy of the authentication but also add to the computing and key-management load—especially at the edge (Hu, 2023).

2.5.3 Revocation and rotation

Revocation rapid propagation is very important (Mazzocca et al., 2024a). On-chain publishing of revocation events enhances transparency; however, their utility relies on how fast gateways/brokers/controllers fetch and implement revocations in the data plane (Abang et al., 2024).

Implication. The "blockchain + smart contracts" solution is just an adjunct, rather than a substitute, for a reliable device identity proofing process, hardware-backed key management, and secure firmware supply chain (Lorych and Plappert, 2024). The allocation of responsibility should be very clear to not give the impression that the net security benefits are overstated (Obaidat et al., 2024) (see Table 2).

3 Comparative analysis of blockchain-based security approaches in IoT

This section synthesizes cross-cutting trade-offs and presents a benchmarking rubric that facilitates evidence-based comparison over diverse IoT environments. In this work, we clarify the differences between on-chain anchors (e.g., audit hashes, revocation notices) and off-chain mandatory controls (device attestation, secure boot, key custody) and analyze the findings considering the identity and trust-chain lifecycle (Section 2.5) (Obaidat et al., 2024; Abang et al., 2024; Tranvåg, 2025; Eghmazi et al., 2024b).

3.1 Non-obvious trade-offs

(1) Decentralization vs. real-time QoS. More validator diversity and on-chain verification can lead better system transparency/non-repudiation; however, these improvements are frequently accompanied with higher end-to-end delays and jitters. Such performance degradations under wireless loss and committee churn can make it difficult for the control loops in Industrial Internet of Things and vehicular applications to operate (Vangala et al., 2022; Abang et al., 2024; Yuan et al., 2025; Banupriya and Sharmila, 2024).

TABLE 1 Comparison of reviewed works.

Authors /year	Domain	Objective	Blockchain/consensus	Evidence	Key results / findings	Limitations	Notes (on/off-chain)
Maeng et al. (2022)	Clustered IoT	Group key management	Hyperledger (permissioned)	Testbed/Prototype	Reduced rekeying overhead; scalable for group comms	Needs broader pilot/real-world validation	On-chain: key events/ audit; Off-chain: device attestation, key custody
Latif et al. (2020)	IIoT (real-time)	Lightweight decentralised architecture	Custom PoAh (per authors)	Prototype	Efficient auth; supports real-time flows	Complexity grows with network size	On-chain: auth anchors; Off-chain: gateways, secure boot
Basudan (2023)	General IoT (high volume)	Scalable tx via group signatures	DABG + group signature	Simulation + Prototype	Batch verification; anonymity and traceability	Sensitive to network instability; privacy↔performance tension	On-chain: tx commitments; Off-chain: ZK/group-sig compute
Oktian et al. (2020)	General / multi-tier	Hierarchical scalable BC	Two-tier hybrid (sub-engine)	Prototype	Parallelism; reduced centralisation; higher throughput	Specialised bridges; interoperability burden	On-chain: tiered policies; Off-chain: protocol gateways
Yang et al. (2021)	General IoT (constrained)	Lightweight mutual auth	Custom BC (lightweight)	Simulation/Testbed	Efficient privacy-preserving auth	Scalability/adaptability under heterogeneity	On-chain: auth logs; Off-chain: device identity proofing
Liu et al. (2023)	Smart home	Privacy + message auth	Consortium BC + IPFS	Prototype	Enhanced privacy; dynamic audits (CLAS sig)	Audit timeliness; precise key lifecycle mgmt	On-chain: audit hashes; Off-chain: payloads/keys (IPFS/HSM)
Kaur and Ali (2021)	General IoT	Integrity + confidentiality	BC + smart contracts + ZKP	Theory + Prototype	Contract-mediated validation; privacy via ZK	Processing overhead/latency vs. real-time	On-chain: proofs/ commitments; Off-chain: ZK generation
Singh et al. (2021)	Survey	Threats/mitigations map	General (PKI/contracts)	Survey	PKI auth; anomaly detection; privacy techniques	Limited empirical validation; zero-day coverage	On-chain: anchors; Off-chain: IDS/ML pipelines
Lahbib et al. (2024)	Survey (trust)	Trust mgmt in BIoT	Reputation/distributed	Survey	Reputation + contracts; aggregation models	Scalability; AI integration; interoperability	On-chain: trust state; Off-chain: signals/features
Vangala et al. (2022)	Vehicular / mobile IoT	Secure key agreement	Hybrid BC, PBFT	Prototype	Dynamic node support; better anonymity	High compute/communication cost	On-chain: session state; Off-chain: cryptographic heavy-lifting
Barazanchi and Hashim (2023)	General IoT	Decentralised IoT security	BC + contracts	Prototype	Device auth; integrity; decentralised comms	Consensus optimisation needed	On-chain: policy/audit; Off-chain: device attestation
Pathak et al. (2023)	Edge IoT	Trust-based access control	Hyperledger; ABAC contracts	Prototype	End-to-end security; TCC contracts	Sidechains; trust-model refinement	On-chain: ABAC decisions; Off-chain: PDP/ PEP details

(Continued)

10.3389/fcomp.2025.1670473

TABLE 1 (Continued)

Authors /year	Domain	Objective	Blockchain/consensus	Evidence	Key results / findings	Limitations	Notes (on/off-chain)
Liu et al. (2020)	General Edge	Decentralised access control (fabric-iot)	Hyperledger Fabric	Prototype	Fine-grained ABAC via contracts	Mobility/resource issues; limited generalisability	On-chain: access logs; Off-chain: identity proofing
Shammar et al. (2021)	Survey	BIoT security review	Lightweight/off-chain/layered	Survey	Advocates layered/off-chain crypto	Edge integration; light protocols needed	On-chain: anchors; Off-chain: lightweight crypto at edge
Shammar et al. (2022)	General IoT	ABAC via Hyperledger	Hyperledger Fabric	Prototype	Decentralised ABAC; reduced latency	Real devices; multi-org testing	On-chain: ABAC policy; Off-chain: org governance
Seshadri et al. (2020)	Constrained IoT	Malicious IoT monitoring	Hyperledger Fabric	Prototype	HW add-ons; latency reduction	Scalability; diversity of systems	On-chain: events; Off-chain: HW root of trust
Anjum et al. (2025)	Healthcare	Opportunistic access control	BC + ML + contracts	Prototype (clinical context)	Contextual, real-time access; delegation	ML tuning/monitoring overhead	On-chain: decisions/audit; Off-chain: features/model
Gong et al. (2021)	General IoT	Device identity auth	IoT BC + BCoT Gateway	Prototype	Traffic-flow auth; scalable with feature selection	Real deployment pending; dynamic features	On-chain: auth records; Off-chain: gateway features
Rathee et al. (2022)	IIoT	Trust mgmt + secure tx	BC + trust computation	Prototype	Improved secure transmission; trust model	Coordinator bottlenecks/risks	On-chain: trust ledger; Off-chain: coordinators
Janani and Ramamoorthy (2023)	General IoT	Device identity and access	Hyperledger; PIoT + ECDSA	Prototype	Strong auth and access control	Flexibility; real-world efficacy	On-chain: policy/audit; Off-chain: device attestation
Alzoubi et al. (2022)	Survey	Integration challenges	Layered/fog/BC	Survey	Edge/fog BC; off-chain and lightweight	Standardisation; new platforms	On-chain: anchors; Off-chain: fog/edge crypto
Ramezan and Meamari (2024a)	General IoT	ZKPs for firmware/data	zk-IoT (Groth16/Plonk)	Prototype/Theory	Privacy + tamper evidence	High computation; latency; scalability	On-chain: proof verify; Off-chain: proof gen
Ruzbahani (2024)	General IoT	AI-protected security/privacy	BC + AI + contracts	Prototype	AI anomaly detection; privacy	Integration complexity; ethics/regulation	On-chain: audit; Off-chain: AI pipeline
Gopalan et al. (2024)	General IoT	Deauth mitigation	BC + ECDSA + MTT	Prototype/Testbed	94–98% accuracy; real-time robust	Real-time deployment maturity	On-chain: incident hashes; Off-chain: RF/ML
Lee et al. (2023)	General IoT	Data access + mutual auth	BC + CP-ABE	Prototype/Formal	Fine-grained access; auditability	ABE cost; key-lifecycle complexity	On-chain: policy logs; Off-chain: key custody
Natraj et al. (2025)	Resource-limited IoT	Lightweight data mgmt	Lightweight consensus + batching	Simulation/Prototype	High throughput; error handling	Consensus tuning; IoT-specific tailoring	On-chain: state commits; Off-chain: device crypto
Zhao et al. (2024)	IIoT	Lightweight auth (secure)	LRBCM, ELAM (ECC-based)	Prototype	Reputation-aided consensus; energy efficient	Consensus scalability; evolving threats	On-chain: reputation/ledgers; Off-chain: ECC ops

(Continued)

10.3389/fcomp.2025.1670473

TABLE 1 (Continued)

Authors /year	Domain	Objective	Blockchain/consensus	Evidence	Key results / findings	Limitations	Notes (on/off-chain)
Yang et al. (2021)	General IoT	Decentralised mutual auth	BC + MSR crypto	Prototype	Reduced overhead; scalable auth	Privacy/overhead trade-offs	On-chain: auth anchors; Off-chain: MSR compute
Barazanchi and Hashim (2023)	General IoT	Decentralised security framework	PoS + BFT-inspired	Prototype	Lower energy; access control	Consensus optimisation; deployment	On-chain: access logs; Off-chain: device trust
Ragul et al. (2025)	General IoT	Dynamic trust evaluation	BC + ABAC + ECDSA	Prototype/Simulation	Continuous trust; anomaly detection	ML/crypto integration; deployment	On-chain: trust/ABAC; Off-chain: anomaly models
Eghmazi et al. (2024a)	Smart city and IIoT	Multi-layer scalable IoT	Hyperledger Fabric + Kafka	Prototype/Pilot	Handles dynamic volumes; strict access	Integration overhead; infra cost	On-chain: access/audit; Off-chain: Kafka streams
Obaidat et al. (2024)	Cross-domain (Survey)	Opportunities, challenges, applications	General (survey)	Survey	Synthesises BIoT benefits/limits; stresses domain-specificity and integration overhead	Limited empirical evaluation by design	On-chain: anchors; Off-chain: device identity/attestation
Abang et al. (2024)	Performance/IIoT	Latency modelling (HLF)	Hyperledger Fabric	Modelling/Exp.	Highlights p95/p99 tails; ordering/gateway settings dominate latency	Fabric-specific; setup sensitivity	On-chain: block/order params; Off-chain: gateway/broker bottlenecks
Tranvåg (2025)	Data anchoring	Benchmarking IPFS↔Ethereum anchoring	Ethereum + IPFS	Benchmark/Design	Quantifies storage/event and gas; shows selective anchoring patterns	Platform-specific; pinning assumptions	On-chain: commitments; Off-chain: payloads (IPFS)
Yuan et al. (2025)	Consensus (Survey)	PBFT evolution/optimisation	PBFT family	Survey	Analyses quadratic messaging, view-change, parameter tuning	Survey scope; not device-level	On-chain: finality rules; Off-chain: committee ops/tooling
Banupriya and Sharmila (2024)	Consensus tuning	Improve PBFT-like finality at scale	PBFT-like	Experimental/Analysis	Parameter optimisation reduces latency under load	Generalisability to heterogeneous IoT unclear	On-chain: consensus events; Off-chain: deployment tuning
Hu (2023)	Access control (ABE)	Practical considerations for ABE	ABE guidance	Standards/Guidance	Details key lifecycle, policy granularity, overheads	Not IoT-specific evaluation	On-chain: policy logs; Off-chain: key custody/HSM
Yang et al. (2024)	Data access control	ABE with blockchain	CP-ABE + BC	Protocol/Eval	Demonstrates fine-grained control with BC integration	Resource/latency overhead on devices	On-chain: access decisions; Off-chain: ABE compute
Mahdavi et al. (2024)	Crypto offload	IoT-friendly outsourced ABE	Outsourced ABE	Protocol/Eval	Offloading reduces device cost via precomputation	Trust in proxy; complexity	On-chain: proofs/receipts; Off-chain: ABE proxy
Wu et al. (2024)	Data sharing	ABE in BC environments	CP-ABE + BC	System/Analysis	Integrates ABE with BC for controlled sharing	Storage/latency trade-offs	On-chain: policy anchors; Off-chain: ciphertexts/keys
Ramezan and Meamari (2024a)	Privacy/ZK	zk-IoT for firmware/data	ZKPs + BC	Theory/Prototype	Strengthens confidentiality + tamper evidence	High compute/latency on edges	On-chain: verify; Off-chain: proof generation

(Continued)

10.3389/fcomp.2025.1670473

TABLE 1 (Continued)

Authors /year	Domain	Objective	Blockchain/consensus	Evidence	Key results / findings	Limitations	Notes (on/off-chain)
Zhou et al. (2024)	Identity privacy	ZK for identity sharing	ZK + BC	Protocol/Analysis	Private identity assertions with auditability	Prototype-level; integration pending	On-chain: proof records; Off-chain: identity providers
Mazzocca et al. (2024b)	Decentralised identity	DIDs and VCs landscape	DID/VC	Survey	Maps threats, ecosystems, adoption hurdles	Limited deployment metrics	On-chain: credential status; Off-chain: issuance/ holders
Lorych and Plappert (2024)	Hardware trust	HW trust anchors for updatable IoT	Attestation/Measured boot	System/Prototype	Anchors identity/firmware trust off-chain	Hardware rollout/ops cost	On-chain: attestation results; Off-chain: TPM/ TEE
Mazzocca et al. (2024b)	Revocation at scale	Efficient VC revocation (IoT)	VC/Revocation	USENIX Security	Fast revocation with measured propagation	VC-specific; network dependency	On-chain: revocation notices; Off-chain: distribution
El-Hajj and Beune (2024)	Lightweight PKI	Zone-based PKI for IoT	Decentralised PKI	System/Analysis	Localised trust reduces overhead; scalable zones	Zone mgmt complexity	On-chain: registry/CRL; Off-chain: enrolment/ attestation
Gopalan et al. (2024)	Wireless security	Deauthentication mitigation	BC + ECDSA + MTT	Testbed	94–98% detection; robust in real time	Deployment maturity; data drift	On-chain: incident hashes; Off-chain: RF/ML pipeline
Kim and Kim (2024)	Wireless resilience	Jamming impact on BC-based distributed learning	BC + DL	Simulation/Analysis	Shows disruptive jamming risks to BC/DL loops	Domain generality; mitigation external	On-chain: audit anchors; Off-chain: RF monitoring

10.3389/fcomp.2025.1670473

(2) Strong privacy vs. device budget. To achieve better privacy and policy fidelity, zero-knowledge proofs and CP-ABE are used, but as a result, they raise the amount of computation, memory, and key-lifecycle overhead on constrained nodes. Hybrid off-chain verification can lessen the device load; however, it goes a step further to re-introduce trusted components (Hu, 2023; Yang et al., 2024; Mahdavi et al., 2024; Wu et al., 2024; Ramezan and Meamari, 2024b; Zhou et al., 2024).
(3) Generalizability vs. domain fit. Domain-specific (healthcare, smart home, industrial) tailored frameworks are likely to be very successful locally, nevertheless, they make certain assumptions about traffic patterns, risk models, and trust anchors that gradually erode their ability to be scalable and portable across different regions and jurisdictions; the majority of the support for this claim comes from prototypes/pilots rather than production deployments (Liu et al., 2023; Anjum et al., 2025; Rathee et al., 2022; Obaidat et al., 2024; Eghmazi et al., 2024b).

3.2 Benchmarking rubric for BIoT security solutions

Comparisons are conducted using five axes, we "benchmark" solutions by specifying at least one metric for each of the axes:

- Security: policy-enforcement correctness; safety/liveness under churn; MTTD/MTTR; revocation effectiveness (Obaidat et al., 2024; Mazzocca et al., 2024a).
- Performance: latency; effective throughput under bursts; view-change/leader-election cost (relevant for PBFT-like finality) (Abang et al., 2024; Yuan et al., 2025; Banupriya and Sharmila, 2024).
- Resource: energy per transaction; CPU/RAM/flash footprints; storage growth per anchored event (esp. with selective anchoring) (Abang et al., 2024; Tranvåg, 2025; Eghmazi et al., 2024b; Hu, 2023; Yang et al., 2024; Mahdavi et al., 2024; Wu et al., 2024; Ramezan and Meamari, 2024b).
- Governance: revocation propagation latency; key/credential rotation SLAs; committee rotation cadence (Obaidat et al., 2024; Mazzocca et al., 2024a).
- Interoperability: gateway failure modes; protocol coverage; portability across vendors/jurisdictions (on−/off-chain split) (Obaidat et al., 2024; Abang et al., 2024; Tranvåg, 2025; Eghmazi et al., 2024b).

In such cases, the recommendation would be to log consensus-critical events as on-chain attestations while keeping heavy cryptography and payloads off-chain (Abang et al., 2024; Tranvåg, 2025; Eghmazi et al., 2024b; Ramezan and Meamari, 2024b).

3.3 Interdependency framework

Challenges in BIoT are causally interdependent; alleviating one can follow another that is worse. We are recommending a conceptual model that charts primary drivers—Resource Constraints, Latency/Throughput, Identity Governance, Privacy Requirements, Domain Assumptions—to their results—Security Posture, Scalability, Portability (Obaidat et al., 2024; Abang et al., 2024; Tranvåg, 2025; Eghmazi et al., 2024b; Hu, 2023; Yang et al., 2024; Mahdavi et al., 2024; Wu et al., 2024; Ramezan and Meamari, 2024b; Zhou et al., 2024; Mazzocca et al., 2024a) (see Table 3).

3.4 Practical implementation and benchmarking challenges

Most assessments are still experimental stages/pilots; the transition to diverse, production-grade ecosystems entails: workload-realistic experiments (burst traffic, partial synchrony, adversarial churn, RF loss/jamming) (Abang et al., 2024; Yuan et al., 2025; Banupriya and Sharmila, 2024; Kim and Kim, 2024); lifecycle authenticity (issuance/rotation/revocation at scale; supply-chain variance) (Mazzocca et al., 2024a,b; Lorych and Plappert, 2024); operational cost measuring (SRE effort, incident response, audit pipelines, data-residency compliance) (Obaidat et al., 2024; Abang et al., 2024; Tranvåg, 2025; Eghmazi et al., 2024b); and reporting practice (publish p95 latency and energy/tx; disclose off-chain dependencies; include failure-mode analysis) (Abang et al., 2024; Tranvåg, 2025; Eghmazi et al., 2024b; Hu, 2023; Yang et al., 2024; Mahdavi et al., 2024; Wu et al., 2024; Ramezan and Meamari, 2024b; Zhou et al., 2024).

3.5 Synthesis matrix: comparative summary of blockchain-IoT approaches

Table 4 shows comparative summary of blockchain-IoT security approaches. This synthesis matrix categorizes representative studies by theme (authentication, privacy, scalability, and AI-driven trust), highlighting reported benefits, limitations, and target IoT domains. Claims on privacy/auditability should be interpreted alongside: (i) p95 latency under bursty workloads, (ii) energy per transaction, (iii) revocation-propagation latency, and (iv) the on-/off-chain responsibility split, before cross-domain comparisons are made (Abang et al., 2024; Tranvåg, 2025; Eghmazi et al., 2024b; Yuan et al., 2025; Ramezan and Meamari, 2024b; Mazzocca et al., 2024a).

4 Challenges in current research

Recent literature Maeng et al. (2022), Latif et al. (2020), Basudan (2023), Oktian et al. (2020), Yang et al. (2021), Liu et al. (2023), Kaur and Ali (2021), Singh et al. (2021), Lahbib et al. (2024), Vangala et al. (2022), Barazanchi and Hashim (2023), Pathak et al. (2023), Liu et al. (2020), Shammar et al. (2021, 2022), Seshadri et al. (2020), Anjum et al. (2025), Gong et al. (2021), Rathee et al. (2022), Janani and Ramamoorthy (2023), Alzoubi et al. (2022), Ramezan and Meamari (2024a,b), Ruzbahani (2024), Gopalan et al. (2024), Lee et al. (2023), Natraj et al. (2025), Zhao et al. (2024), Yang et al. (2021), Barazanchi and Hashim (2023), Ragul et al. (2025), Eghmazi et al. (2024a,b), Obaidat et al. (2024), Abang et al. (2024), Tranvåg (2025), Yuan et al. (2025), Banupriya and Sharmila (2024), Hu (2023), Yang et al. (2024), Mahdavi et al. (2024), Wu et al. (2024), Zhou et al. (2024), Mazzocca et al. (2024a,b), Lorych and Plappert (2024), El-Hajj and Beune (2024), Gopalan et al. (2024), and Kim and Kim (2024) reveals that,

TABLE 2 The mapping of IoT attack vectors to on-chain BIoT controls, off-chain dependencies, and practical limits.

Attack vector	On-chain BIoT controls	Off-chain dependencies	Limits	Refs
Device spoofing/Sybil	PKI registries; stake/trust-weighted admission	Secure enrolment; supply-chain attestation	Registry ≠ identity proof	Gong et al. (2021), Liu et al. (2020), Pathak et al. (2023), El-Hajj and Beune (2024), Mazzocca et al. (2024b), Lorych and Plappert (2024), and Obaidat et al. (2024)
MITM/replay	Signed telemetry; nonce/timestamps anchored	Time synchronisation; key rotation	Clock drift; storage growth for anchors	Kaur and Ali (2021), Yang et al. (2021), Liu et al. (2023), Barazanchi and Hashim (2023), Abang et al. (2024), Tranvåg (2025), and Obaidat et al. (2024)
Firmware tampering	Notarised attestation results (hash anchoring)	Measured boot; TPM/TEE oracles	Oracle trust/availability	Ramezan and Meamari (2024a), Seshadri et al. (2020), Lorych and Plappert (2024), and Tranvåg (2025)
Deauthentication/jamming	Incident notarisation; policy triggers	RF monitoring; IDS/ML	Mitigation remains physical / off-RF	Gopalan et al. (2024), Ruzbahani (2024), Kim and Kim (2024), and Obaidat et al. (2024)
Key compromise	Rapid on-chain revocation; rotation logs	HSM; policy distribution	Propagation latency to gateways/controllers	Maeng et al. (2022), Lee et al. (2023), Janani and Ramamoorthy (2023), Mazzocca et al. (2024a), Lorych and Plappert (2024), and Abang et al. (2024)
Data tampering	Append-only audit trails; state commitments	Reliable off-chain storage	Throughput/latency trade-offs	Barazanchi and Hashim (2023), Kaur and Ali (2021), Singh et al. (2021), Eghmazi et al. (2024a), Tranvåg (2025), and Abang et al. (2024)
Privilege abuse	Policy-change logging via smart contracts	External PDP/PEP; approval workflows	Human factors; contract bugs	Shammar et al. (2022), Pathak et al. (2023), Barazanchi and Hashim (2023), Liu et al. (2020), and Obaidat et al. (2024)
Privacy leakage	Selective anchoring; ZKPs when feasible	Off-chain payload stores; DLP controls	ZK/ABE compute cost on edge	Liu et al. (2023), Kaur and Ali (2021), Lee et al. (2023), Ramezan and Meamari (2024a,b), Hu (2023), Yang et al. (2024), Wu et al. (2024), Mahdavi et al. (2024), and Obaidat et al. (2024)

The figure specifies for each row the security controls, required off-chain enablers (e.g., enrolment/attestation, PDP/PEP, HSM/TPM/TEE), as well as known constraints, along with citations chosen from basic and latest research works to support the deployment context.

notwithstanding the blockchain integration leading to the offering of several advantages for the IoS ecosystems, there are still many unresolved critical challenges. These issues become even more complicated with new architectures, advanced cryptography, and cross-disciplinary integrations (e.g., AI-blockchain). The principal barriers are outlined in Figure 2.

This figure depicts the largest impediments derived from the analysed papers—covering scalability, resource constraints, security weaknesses, privacy protection, consensus feasibility/performance, data integrity, interoperability, regulatory compliance, environmental impact, and usability (Maeng et al., 2022; Latif et al., 2020; Basudan, 2023; Oktian et al., 2020; Yang et al., 2021; Liu et al., 2023; Kaur and

TABLE 3 Interdependency matrix for BIoT challenges (drivers → direct effects → impacted dimensions).

Driver	Direct effect	Impacted dimension
Resource constraints	Weak keys, less frequent attestation	Security weaknesses
Resource constraints	High crypto load	Latency, throughput, scalability
Privacy requirements	Heavy ZKP/ABE compute	Latency and energy overhead
Identity and governance	Revocation/rotation dependencies	Trust assurance, portability
Domain assumptions	Narrow traffic/risk model	Portability, generalizability
Scalability bottlenecks	Failover risks, consensus fragility	Security guarantees

Rows encode causal links from each driver to its immediate effect and the affected security/performance dimensions.

Ali, 2021; Singh et al., 2021; Lahbib et al., 2024; Vangala et al., 2022; Barazanchi and Hashim, 2023; Pathak et al., 2023; Liu et al., 2020; Shammar et al., 2021, 2022; Seshadri et al., 2020; Anjum et al., 2025; Gong et al., 2021; Rathee et al., 2022; Janani and Ramamoorthy, 2023; Alzoubi et al., 2022; Ramezan and Meamari, 2024a,b; Ruzbahani, 2024; Gopalan et al., 2024; Lee et al., 2023; Natraj et al., 2025; Zhao et al., 2024; Yang et al., 2021; Barazanchi and Hashim, 2023; Ragul et al., 2025; Eghmazi et al., 2024a,b; Obaidat et al., 2024; Abang et al., 2024; Tranvåg, 2025; Hu, 2023; Yang et al., 2024; Mahdavi et al., 2024; Wu et al., 2024; Zhou et al., 2024; Mazzocca et al., 2024a; Kim and Kim, 2024).

4.1 Scalability

The diverse and rapidly increasing number of IoT nodes, as well as the high frequency of telemetry, are the reasons why scalability is the main concern. Throughput can be raised by conventional and hierarchical designs; however, performance limits can be still observed under industrial-scale workloads and partial synchrony (Latif et al., 2020; Oktian et al., 2020; Natraj et al., 2025; Eghmazi et al., 2024a; Abang et al., 2024; Yuan et al., 2025; Banupriya and Sharmila, 2024). As an illustration, Natraj et al. (2025) cite the case of throughput escalation in lightweight designs, yet at the point where the system is scaled up, bottlenecks reappear. Layered or Kafka-backed stacks (Eghmazi et al., 2024a,b; Abang et al., 2024) can alleviate the problem, but they also suffer from the issue of having to do proper capacity planning and back-pressure control.

4.2 Resource constraints

IoT devices have strict limitations in budgets (CPU/RAM/flash/energy). Lightweight consensus and authentication are considered the right track (Yang et al., 2021; Natraj et al., 2025; Zhao et al., 2024; Yang et al., 2021), however, there is still the security–resource trade-off problem, which is even more aggravated by heterogeneous links and burst loads (Hu, 2023; Yang et al., 2024; Mahdavi et al., 2024; Wu et al., 2024). Take for example Yang et al. (2021) who utilize modular square-root crypto to lessen computation, but at the expense of long-term cryptographic strength.

4.3 Security weaknesses

In their essence, blockchains allow tamper-evident logging; however, in a real-world scenario, certain weaknesses emerge due to the interactions between humans and technical systems - theft of keys, compromise of firmware, misconfiguration, etc. (Yang et al., 2021; Gong et al., 2021; Ramezan and Meamari, 2024a; Gopalan et al., 2024; Lee et al., 2023; Yang et al., 2021; Ragul et al., 2025). Mitigating actions (for instance, AI-assisted detection, policy automation), if performed in real-time, may result in oversubscription of the resources of a device and thus, the arising of the operational complexity (Ramezan and Meamari, 2024a; Gopalan et al., 2024; Ragul et al., 2025). As an example, Gopalan et al. (2024) combine blockchain with multi-task transformers for real-time deauthentication detection. However, the device/edge cost still needs to be scheduled.

4.4 Privacy protection

The main characteristics of blockchains, i.e., transparency and immutability, somehow contradict with the principle of data minimization. Zero-knowledge proofs (ZKPs) (Ramezan and Meamari, 2024a,b; Zhou et al., 2024), ciphertext-policy attribute-based encryption (CP-ABE) (Lee et al., 2023; Hu, 2023; Yang et al., 2024; Mahdavi et al., 2024; Wu et al., 2024), and selective anchoring (hash on-chain, payload off-chain) (Eghmazi et al., 2024a,b; Abang et al., 2024; Tranvåg, 2025) enhance privacy, but at the same time, these techniques entail longer computation times, more complex integration efforts, and more challenging key-lifecycle management. For instance, Ramezan and Meamari (2024a) (zk-IoT) make use of ZKPs to grant data confidentiality for firmware and data integrity, however, taking the majority of the costs in the proof.

4.5 Consensus and transaction processing (feasibility, performance, and energy)

Traditional PoW/PoS are not very effective for constrained IoT scenarios (Vangala et al., 2022; Janani and Ramamoorthy, 2023; Natraj et al., 2025; Zhao et al., 2024; Barazanchi and Hashim, 2023). PBFT-like finality offers better latency at small committees but encounters quadratic messaging and view-change overheads with scale/churn increase (Yuan et al., 2025; Banupriya and Sharmila, 2024; Abang et al., 2024). Reputation-supported or lightweight variations lessen the volume of chatter (Natraj et al., 2025; Zhao et al., 2024; Barazanchi and Hashim, 2023), however, they can become less secure in terms of partitions/Byzantine behavior or rely on fragile trust assumptions (Zhao et al., 2024; Barazanchi and Hashim, 2023). Moreover, energy/green-computing limitations further restrict the option, especially for battery-powered nodes (Natraj et al., 2025; Zhao et al., 2024; Barazanchi and Hashim, 2023; Abang et al., 2024).

TABLE 4 Comparative summary of blockchain-IoT approaches.

Theme	Key papers	Benefits	Drawbacks	Target IoT domain	Notes
Authentication and access control	Maeng et al. (2022), Yang et al. (2021), Vangala et al. (2022), Pathak et al. (2023), Liu et al. (2020), Gong et al. (2021), Lee et al. (2023), Zhao et al. (2024), and Yang et al. (2021)	Decentralised, fine-grained control; mutual authentication; auditable grants/denials	Key-lifecycle complexity; view-change/committee overhead; gateway offload often required (Abang et al., 2024; Yuan et al., 2025)	IIoT, Edge, Cross-domain, General	On-chain: policy/audit anchors Off-chain: device identity proofing, PDP/PEP (Obaidat et al., 2024; Lorych and Plappert, 2024)
Privacy and data integrity	Liu et al. (2023), Kaur and Ali (2021), Singh et al. (2021), Ramezan and Meamari (2024a), Ruzbahani (2024), Lee et al. (2023), Yang et al. (2021), and Eghmazi et al. (2024a)	ZKP/CP-ABE: stronger privacy; immutable state; non-repudiation	Compute/latency overhead; potential auditability gaps if payloads encrypted off-chain Hu (2023), Yang et al. (2024), Mahdavi et al. (2024), Wu et al. (2024), Ramezan and Meamari (2024b), and Zhou et al. (2024)	Sensitive/regulated IoT, healthcare, smart cities	Selective anchoring; disclose proof/verify costs (Abang et al., 2024; Tranvåg, 2025; Eghmazi et al., 2024b; Ramezan and Meamari, 2024b)
Scalability and lightweight design	Latif et al. (2020), Oktian et al. (2020), Natraj et al. (2025), Zhao et al. (2024), Yang et al. (2021), Barazanchi and Hashim (2023), and Eghmazi et al. (2024a)	Higher throughput; lower per-tx cost; lighter committees	Reduced resilience to churn/partitions; bridge complexity (Abang et al., 2024; Yuan et al., 2025; Banupriya and Sharmila, 2024)	Industrial, sensor nets, large-scale IoT	Tune committee size/timeouts; test under partial synchrony (Abang et al., 2024; Yuan et al., 2025)
AI-driven security and trust management	Lahbib et al. (2024), Anjum et al. (2025), Ruzbahani (2024), Gopalan et al. (2024), Ragul et al. (2025), and Eghmazi et al. (2024a)	Proactive/adaptive defence; dynamic trust; anomaly detection	Integration complexity; model drift and governance (data/feature quality) (Obaidat et al., 2024; Kim and Kim, 2024)	Adaptive, autonomous, critical IoT	Combine on-chain audit with off-chain AI pipelines (Obaidat et al., 2024; Abang et al., 2024; Tranvåg, 2025; Eghmazi et al., 2024b)

Situation: Zhao et al. (2024)'s LRBCM reduces energy consumption, however, it can be impacted negatively by the adversarial setting; Barazanchi and Hashim (2023) utilizes PoS/BFT for the purpose of efficiency, but the security of the system is only guaranteed partially under concentration/partitions.

4.6 Data quality and integrity

Classic PoW/PoS are not favorable for constrained IoT (Vangala et al., 2022; Janani and Ramamoorthy, 2023; Natraj et al., 2025; Zhao et al., 2024; Barazanchi and Hashim, 2023). PBFT-like finality allows faster response time at small committees but due to quadratic messaging and view-change overheads as scale/churn increase, it is not suitable for large networks (Yuan et al., 2025; Banupriya and Sharmila, 2024; Abang et al., 2024). Reputation-supported or lightweight versions help in reducing the number of messages (Natraj et al., 2025; Zhao et al., 2024; Barazanchi and Hashim, 2023), nonetheless, they can be less robust against network partitions/Byzantine behaviors or rely on trust assumptions which are not completely secure (Zhao et al., 2024; Barazanchi and Hashim, 2023). Besides, energy/green-computing limitations narrow the selection even more, in particular, for battery-powered nodes (Natraj et al., 2025; Zhao et al., 2024; Barazanchi and Hashim, 2023; Abang et al., 2024). For instance: Zhao et al. (2024)'s LRBCM cuts down power consumption, however, it can be compromised in the presence of adversaries; Barazanchi and Hashim (2023) uses PoS/BFT to achieve energy efficiency, though the security is not guaranteed under concentration/partition scenarios.

4.7 Interoperability and integration complexity

Protocol diversity and vendor heterogeneity inflate integration cost. Hierarchical/multi-layered stacks offer flexibility (Liu et al., 2020; Eghmazi et al., 2024a) but introduce specialised bridges and lifecycle overhead (Eghmazi et al., 2024a,b). Portability often degrades when domain-specific assumptions seep into core architecture (Obaidat et al., 2024; Eghmazi et al., 2024b).

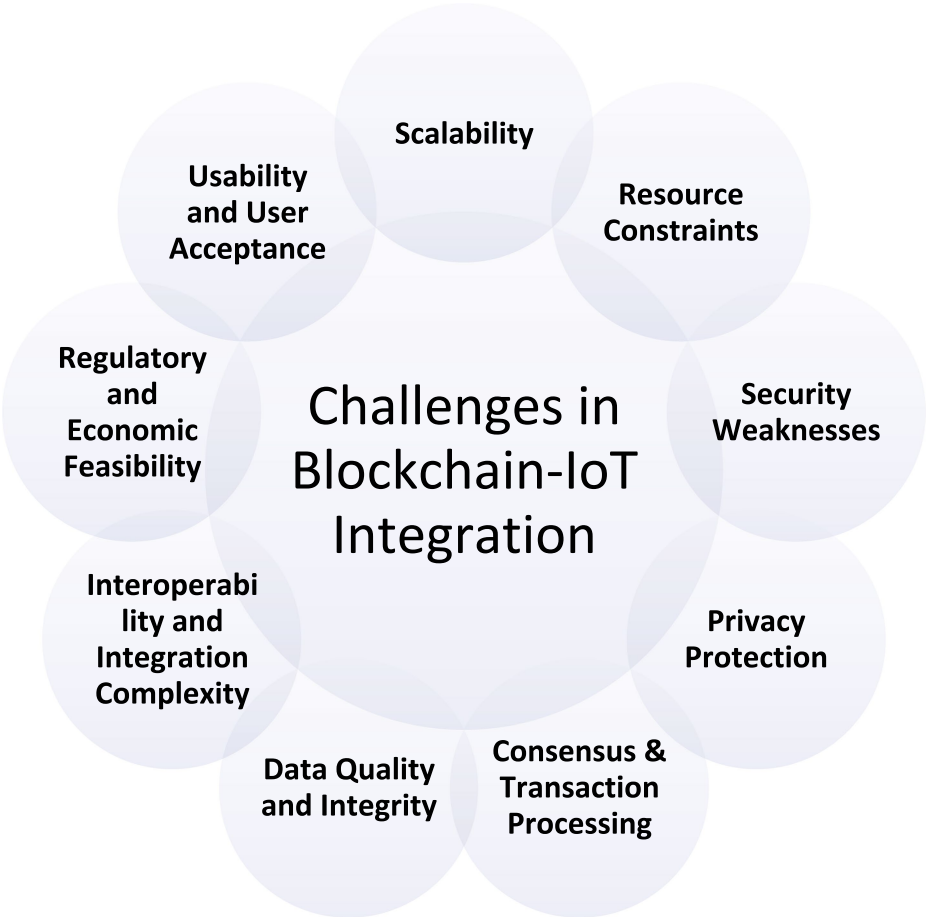

FIGURE 2
Key research challenges in blockchain-IoT integration.

4.8 Regulatory and economic feasibility

Compliance (privacy, data residency, sectoral rules) constrains architecture choices (Ruzbahani, 2024; Eghmazi et al., 2024a,b; Obaidat et al., 2024; Abang et al., 2024; Tranvåg, 2025). Compliance-by-design pushes auditable controls and selective anchoring (Abang et al., 2024; Tranvåg, 2025; Eghmazi et al., 2024b), while identity governance and revocation propagation become measurable obligations (Mazzocca et al., 2024a). Economic viability hinges on SRE effort, incident response, audit pipelines, and integration cost (Obaidat et al., 2024; Abang et al., 2024; Tranvåg, 2025; Eghmazi et al., 2024b). Ethical/legal gaps around AI–blockchain are highlighted in (Ruzbahani, 2024).

4.9 Usability and user acceptance

Complex stacks negatively affect the usability of the operators and users who are, therefore, less willing to use them, especially in the case of consumer IoT. Such systems need simpler interfaces with explicit failure modes that do not undermine the level of trust (Barazanchi and Hashim, 2023; Eghmazi et al., 2024a; Obaidat et al., 2024). For instance: Eghmazi et al. (2024a) recognize the issue of usability impacting the implementation of multi-layer solutions as a "practical hurdle."

5 Solution identification and future research

The comparative analysis (Maeng et al., 2022; Latif et al., 2020; Basudan, 2023; Oktian et al., 2020; Yang et al., 2021; Liu et al., 2020, 2023; Kaur and Ali, 2021; Singh et al., 2021; Lahbib et al., 2024; Vangala et al., 2022; Barazanchi and Hashim, 2023; Pathak et al., 2023; Shammar et al., 2021, 2022; Seshadri et al., 2020; Anjum et al., 2025; Gong et al., 2021; Rathee et al., 2022; Janani and Ramamoorthy, 2023; Alzoubi et al., 2022; Ramezan and Meamari, 2024a,b; Ruzbahani, 2024; Gopalan et al., 2024; Lee et al., 2023; Natraj et al., 2025; Zhao et al., 2024; Yang et al., 2021; Barazanchi and Hashim, 2023; Ragul et al., 2025; Eghmazi et al., 2024a,b; Obaidat et al., 2024; Abang et al., 2024; Tranvåg, 2025; Yuan et al., 2025; Banupriya and Sharmila, 2024; Hu, 2023; Yang et al., 2024; Mahdavi et al., 2024; Wu et al., 2024; Zhou et al., 2024; Mazzocca et al., 2024a,b; Lorych and Plappert, 2024; El-Hajj and Beune, 2024; Gopalan et al., 2024; Kim and Kim, 2024) was instrumental in the understanding the design principles outlined in this section as well as identifying the

research directions related to these challenges. These difficulties pertain to the combination of blockchain and IoT. Consequently, the need arises to dwell on these four aspects, namely, uncomplicatedness, scalability, privacy by design, and the possibility of functioning in a diverse and resource-limited environment.

5.1 Modular and responsibility-aware architectures

Identity management, authentication, access control, and data integrity need to be separated into clearly defined components for future systems to be layered modularity. By using so-called selective anchoring that allows for the placing of a hash and attestations on-chain while the main data and cryptography remain off-chain, one can achieve a good balance between the system's verifiability and its efficiency (Eghmazi et al., 2024a,b; Abang et al., 2024; Tranvåg, 2025). Moreover, this kind of modularity lowers the system's architectural complexity, makes upgrades easier, and limits the extent to which failures can affect the system.

5.2 Consensus mechanisms for realistic deployment

Lightweight and parameterised consensus protocols need to be congruent with the actual conditions in which they operate in the world. This means that they must be able to handle network irregularities, device heterogeneity, and energy constraints. Such an assessment should go beyond the typical computer simulations, including latency, throughput under burst loads, and resilience to churn and partitions (Abang et al., 2024; Yuan et al., 2025; Banupriya and Sharmila, 2024).

Deterministic trust scoring combined with BFT-style finality is a hybrid model that has the potential to provide a desirable compromise between energy efficiency and resilience (Zhao et al., 2024; Barazanchi and Hashim, 2023). Nevertheless, they also have to be thoroughly tested under harsh conditions like collusion, denial-of-service, and partial synchrony failures (Vangala et al., 2022; Natraj et al., 2025; Abang et al., 2024).

5.3 Privacy-preserving but resource-conscious approaches

Confidentiality-preserving methods like zero-knowledge proofs (ZKPs) and ciphertext-policy attribute-based encryption (CP-ABE) offer almost foolproof privacy guarantees (Ramezan and Meamari, 2024a,b; Lee et al., 2023; Hu, 2023; Yang et al., 2024; Mahdavi et al., 2024; Wu et al., 2024; Zhou et al., 2024), however, the computational and key-management overhead associated with them is usually more than what constrained IoT devices can accommodate. The next work should look into implementing hierarchical or event-triggered programs where complicated cryptographic operations are performed only when the risk level is high. By offloading part of the verification work to the edge or gateway nodes, the device-level burden can be further minimized without losing the quality of the audit.

5.4 Interoperability as a first-class principle

It is necessary that the principle of interoperability is deeply ingrained into the design of the system, instead of being considered as an additional feature. In order for different kinds of vendors, standards, and protocols to be able to exchange information, it is necessary that translation and compatibility layers facilitate such communication (Liu et al., 2020; Eghmazi et al., 2024a,b; Obaidat et al., 2024). Uniform policy schemas and formats of attestation will encourage the free movement of software/hardware across different legal areas and facilitate compliance with regulations without causing any restrictions in the variety of the system.

5.5 Identity governance and revocation

Effective security necessitates that one implements the identity and trust-chain lifecycle: enrolment, issuance, authorisation, logging, revocation, and rotation. Publishing revocation notices on the chain, along with quick distribution at gateways and controllers, gives better confidence (Mazzocca et al., 2024a). The use of DIDs and VCs is a hopeful solution to the problem of identity, if only the part of the key and the attestation that is hardware-based can be trusted (Mazzocca et al., 2024b; Lorych and Plappert, 2024).

5.6 Research agenda: actionable directions

(1) Revocation at scale. Create and evaluate scalable revocation models that have limited propagation delays, and monitor enforcement latency at gateways and controllers (Mazzocca et al., 2024a).
(2) Resource-aware privacy. Facilitate the selective or event-triggered implementation of ZKPs/ABE with verification offloading, and publish the end-to-end latency and energy profiles for representative IoT classes (Hu, 2023; Yang et al., 2024; Mahdavi et al., 2024; Wu et al., 2024; Ramezan and Meamari, 2024b; Zhou et al., 2024).
(3) Consensus under adversity. Experiment with the robustness of lightweight and hybrid consensus protocols under conditions of partial synchrony, RF loss, and adversarial churn, outlining performance tails (Abang et al., 2024; Yuan et al., 2025; Banupriya and Sharmila, 2024; Kim and Kim, 2024).
(4) Selective anchoring patterns. Deliver the code examples for Merkle commitments, hash-chains, and off-chain storage pointers, with the clear and detailed explanation of the trade offs in storage overhead and residency requirements (Eghmazi et al., 2024a,b; Abang et al., 2024; Tranvåg, 2025).
(5) Identity and Attestation Tooling. Establish open testbeds coupling TPM/TEE-based attestation with on-chain notarisation, reporting enrolment, rotation, and revocation times at scale (Lorych and Plappert, 2024; Mazzocca et al., 2024a).
(6) Operational economics. Quantify operational costs (SRE effort, auditing, compliance) and compare total cost of ownership across permissioned, hybrid, and public-anchored deployments (Obaidat et al., 2024; Abang et al., 2024; Tranvåg, 2025; Eghmazi et al., 2024b).

(7) Benchmark suites and public datasets. Release IoT-realistic traces and reproducible benchmarks aligned with the proposed rubric to standardise evaluation practices.

In summary, sustainable blockchain–IoT security solutions should be modular, benchmark-driven, privacy-conscious, and adaptive to dynamic operating conditions. Blockchain can provide verifiable state and programmable auditability, but only when coupled with robust identity governance, effective revocation, and carefully balanced off-chain controls (Obaidat et al., 2024; Abang et al., 2024; Tranvåg, 2025; Eghmazi et al., 2024b; Hu, 2023; Yang et al., 2024; Mahdavi et al., 2024; Wu et al., 2024; Ramezan and Meamari, 2024b; Zhou et al., 2024; Mazzocca et al., 2024a,b; Lorych and Plappert, 2024).

6 Future research directions

The research areas we are outlining here broaden the work from Sections 3–5. They include those aspects that deal with scalability, resource-awareness, privacy-preserving analytics, interoperability, sustainability, and regulation-conscious design in blockchain–IoT systems. The respective research themes are associated with the presented hypotheses and include reporting guidance compliant with the benchmarking rubric from Section 3.2 (e.g., latency, energy/tx, revocation latency).

6.1 Layer-2 and sharding for large-scale IoT

The next step would be to experimentally verify the pointing-out Layer-2 configurations (e.g., rollups, state channels) to keep the throughput levels stable and achieve a reduction in p95 latency in the case of topologies being diverse, say smart factories or cities (Abang et al., 2024). One way to do this is via rollup-based anchoring which effectively sets a limit on storage growth on the chain for each event, at the same time, it allows for full auditability (Tranvåg, 2025). At the same time, it is possible that sharding coupled with locality-aware routing can help maintain throughput levels when there is committee churn and partial synchrony (Yuan et al., 2025; Banupriya and Sharmila, 2024). The burst throughput and different failure scenarios during reorgs/aggregator faults should be a part of disclosures in reports (Abang et al., 2024).

6.2 Context-aware lightweight cryptography

Research is needed on adaptive cryptographic profiles that scale key sizes, proof complexity, and handshake frequency to device context (battery level, link quality, criticality) (Hu, 2023). Event-triggered proofs can meet assurance targets with lower energy per transaction when verification is offloaded to gateways (Ramezan and Meamari, 2024b). CP-ABE and related schemes should be applied selectively on constrained nodes, with explicit reporting of RAM/flash footprints and key-lifecycle overhead (Lee et al., 2023; Hu, 2023; Wu et al., 2024).

6.3 Adaptive trust and reputation models

Trust and reputation should evolve with behavior drift and adversarial activity using supervised/unsupervised/RL methods, while recording on-chain audit anchors for decisions (Obaidat et al., 2024). We hypothesise that adaptive trust improves safety/liveness at fixed communication budgets in PBFT-like settings (Yuan et al., 2025), and that poisoning-resilient designs (e.g., bagging, periodic re-randomisation) limit consensus bias (Kim and Kim, 2024). Authors should report FPR/FNR of detectors and committee-rotation cadence alongside admission latency (Abang et al., 2024).

6.4 Privacy-preserving analytics for sensitive domains

For the healthcare and finance sectors, using federated learning alongside on-chain model-update attestations can lead to the desired accuracy without the need for centralised data pooling (Abang et al., 2024). The selective anchoring of hashes/commitments ensures that there is a record of the auditability while, at the same time, keeping payloads that are off-chain to meet data-residency requirements (Eghmazi et al., 2024a,b). In situations of higher risk, ZKPs and ABE can offer more robust privacy; however, their compute/latency costs still need to be figured out for each device class (Ramezan and Meamari, 2024a,b; Zhou et al., 2024).

6.5 Interoperability standards and cross-platform gateways

Interoperability must be regarded as a constraint of the highest importance, and the adoption of standardised policy schemas (authorisation, attestation) can not only cut down the integration time but also the incident MTTR (Obaidat et al., 2024). The cross-chain gateways can be the connecting point between different vendors and protocols that are incompatible with each other; however, this can only be possible if the interface contracts are formally set so as to avoid any policy ambiguity (Eghmazi et al., 2024b). The ability to move from one jurisdiction/vendor to another should be looked at through repeatable tests (Liu et al., 2020; Eghmazi et al., 2024a).

6.6 Green blockchain architectures for constrained nodes

Battery-powered IoT definitely needs energy-aware consensus (stake/trust-weighted admission + lightweight finality) and duty-cycled participation (Barazanchi and Hashim, 2023). Event batching, properly engineered for commitments, can significantly reduce the

on-chain storage without sacrificing the complete forensics audit trail (Abang et al., 2024). The report should cover energy/tx, leader-election/view-change cost, and auditability under batching (Natraj et al., 2025; Zhao et al., 2024).

6.7 Policy-aware, regulation-responsive design

Architectures need to translate compliance constraints (GDPR, HIPAA, residency) into machine-verifiable policies, on-chain revocation notices, and measurable propagation SLAs for the mitigation of compliance risks (Abang et al., 2024). DIDs/VCs can become a solution for the problem of identity portability across domains if they are accompanied by an efficient revocation mechanism (Mazzocca et al., 2024a,b). The assessment must cover revocation propagation latency and audit time across different legal regimes (Eghmazi et al., 2024a).

6.8 Zero-trust-aligned architectures

Zero-trust alignment assumes breach by default and enforces continuous verification of device identity, posture, and context at each interaction (Obaidat et al., 2024). On-chain policy updates can accelerate consistent enforcement across gateways/controllers, but introduce decision-path latency that must be measured under load (Abang et al., 2024). Experiments should report policy-enforcement correctness under simulated lateral-movement scenarios.

6.9 Post-quantum cryptography readiness

Migration to post-quantum cryptography should leverage hybrid schemes and crypto-agility to preserve compatibility while adding quantum resistance (Hu, 2023). For constrained nodes, the handshake latency/energy and memory footprint of PQC primitives must

TABLE 5 Summary of future research directions.

Direction	Scope (one-liner)	Key hypotheses	Core metrics	Primary risks
L2 and sharding	Improve throughput/latency in industrial/smart-city settings	H1: rollups reduce p95 and storage/event; H2: sharding sustains throughput under churn	p95/p99, burst throughput, storage/event, reorg/aggregator failure modes	Aggregator complexity, reorg handling
Context-aware crypto	Adaptive crypto by battery/link/criticality	H1: event-triggered proofs lower energy/tx; H2: context policies cut handshakes w/o higher MTTR	Energy/tx, RAM/flash, auth success on lossy links, MTTR/MTTD, revocation latency	Policy misconfiguration, heterogeneity
Adaptive trust	Learning-based trust robust to drift/attacks	H1: improves safety/liveness at fixed comms; H2: poisoning-resilient designs limit bias	Safety/liveness under churn, FPR/FNR, comms overhead, rotation cadence	Data bias/drift, poisoning
Privacy-preserving analytics	FL/SMPC/HE with selective anchoring	H1: federated analytics meets accuracy; H2: risk-triggered ZK/ABE meets SLAs	Accuracy vs. p95, energy/tx, drift governance, audit completeness, residency	Crypto/training cost, latency
Interop and gateways	Standard schemas + cross-chain bridges	H1: standardisation reduces integration time/MTTR; H2: formal interfaces reduce ambiguity	Time-to-integrate, gateway failure modes, portability, enforcement correctness	Fragile bridges, vendor lock-in
Green architectures	Energy-aware consensus, batching, duty-cycle	H1: duty-cycling minimises energy/tx with safety; H2: batching cuts storage w/o forensic loss	Energy/tx, duty-cycle, leader-election cost, auditability	Gaps during sleep, evidence granularity
Policy/regulation-aware	Policy-as-code + on-chain revocation	H1: reduces audit effort, preserves traceability; H2: DID/VC revocation improves assurance	Revocation propagation, audit time, legal portability, IR metrics	Evolving regs, compliance load
Zero-trust alignment	Assume breach; continuous verification	H1: cuts lateral movement; H2: on-chain policy updates speed enforcement	Enforcement correctness, rotation effectiveness, decision latency	Added latency, alert fatigue
PQC readiness	Hybrid PQC and crypto-agility	H1: hybrid handshakes keep compatibility + resistance; H2: key-roll preserves trust chain	Handshake latency, energy/tx, RAM/flash, legacy interop	Memory/energy overhead, migration complexity
Open benchmarks	Public suites and realistic traces	H1: standards enable comparability; H2: public datasets accelerate validation	Rubric coverage, reproducibility, scenario diversity	Dataset bias, maintenance burden

be profiled, and key-roll strategies documented to maintain trust-chain continuity (Lorych and Plappert, 2024).

6.10 Open benchmarks and realistic datasets

In order to have a fair and thorough comparison across different studies, it would be beneficial for the community to put out open benchmark suites together with real-life IoT scenarios (bursty traffic, lossy links, adversarial churn) that are in line with the rubric of Section 3.2 (Abang et al., 2024). Public datasets and harnesses not only make it easier for other researchers to replicate the experiments but also expedite the validation process of consensus, privacy, and interoperability protocols (Yuan et al., 2025; Banupriya and Sharmila, 2024).

Table 5 presents summary of future research directions:

7 Conclusion

This paper examines the combined security and privacy challenges of implementing a distributed ledger technology (DLT) solution, specifically blockchain, into the Internet of Things (IoT) environment by critically reviewing and integrating the findings of 31 core studies and other relevant recent works. Although blockchain technology allows for the provision of an accountable state, a logging process that is detectable for any forms of tampering, and programmable policy/audit, its overall advantage is still dependent on the context of the constraints placed on the device budgets, latency/throughput requirements, interoperability, and governance factors. The research findings that have been gathered from various application areas (smart home, healthcare, industrial, and smart city) reveal that improvements in auditability and decentralisation are very often exchanges with the performance, energy, and integration cost, especially in the condition of heterogeneous links and bursty workloads.

The review complements the discussion with three major contributions of his work. The first one is that it differentiates the on-chain anchors (e.g., audit hashes, revocation notices) from off-chain mandatory controls (device identity proofing, secure boot/attestation, key custody), thus giving a clear definition of the boundaries of responsible persons for system assurance. The second one refers to the characteristics of a benchmarking rubric—security, performance, resource efficiency, governance, and interoperability—with concrete reporting baselines (e.g., p95 latency, energy/tx, revocation-propagation latency, storage growth per anchored event) as a means for rigorous cross-study comparison. The third one is the proposal of a challenge interdependency model that depicts the manner in which one dimension (e.g., privacy) may lead to the aggravation of others (e.g., latency and scalability), thus being the reason for the differences in the literature.

The review, looking ahead, describes an outline of possible solutions and an agenda for future research which covers the themes of the modular, responsibility-aware designs, and the practical implementation of operations. The recommended directions include the use of selective anchoring and layered architectures to achieve a compromise between verifiability and efficiency; the evaluation of a lightweight/parameterised consensus under partial synchrony and churn; resource-aware privacy (selective ZK/ABE with offloaded verification); interoperability by design through standardised policy/attestation schemas and robust gateways; besides identity governance, with rapid revocation as the first-class concern.

Moreover, the agenda, which is designed to connect the theory with the practice, also requests the presence of zero-trust-aligned enforcement, readiness for the post-quantum era, and open and reproducible benchmarks with realistic IoT traces. This will allow security and privacy claims to be verified along with cost, latency, and energy under deployment-like conditions.

In essence, the integration of sustainable blockchain and IoT security will not result from a "best" secure design but rather from a combination of (i) a well-defined separation of on-chain and off-chain tasks, (ii) performance measurement based on common metrics, and (iii) privacy-protecting, regulation-compliant, and environment-adaptive solutions. Through the implementation of these principles, initial-stage experiments can transform into systems that are not only efficient with energy, but also certifiable, compatible, and scalable to provide reliable IoT services.

Author contributions

WS: Conceptualization, Formal analysis, Writing – original draft. MA: Conceptualization, Formal analysis, Writing – original draft. SS: Funding acquisition, Project administration, Supervision, Writing – review & editing.

Funding

The author(s) declare that financial support was received for the research and/or publication of this article. This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU 253457).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The authors declare that no Gen AI was used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

References

Abang, J. E., Takruri, H., Al-Zaidi, R., and Al-Khalidi, M. (2024). Latency performance modelling in Hyperledger fabric blockchain: challenges and directions with an IoT perspective. *Internet of Things* 26:101217. doi: 10.1016/j.iot.2024.101217

Alzoubi, Y. I., Al-Ahmad, A., Kahtan, H., and Jaradat, A. (2022). Internet of things and blockchain integration: security, privacy, technical, and design challenges. *Future Internet* 14:216. doi: 10.3390/fi14070216

Anjum, M., Kraiem, N., Min, H., Dutta, A. K., Daradkeh, Y. I., and Shahab, S. (2025). Opportunistic access control scheme for enhancing IoT-enabled healthcare security using blockchain and machine learning. *Sci. Rep.* 15:7589. doi: 10.1038/s41598-025-90908-1

Banupriya, S., and Sharmila, P. (2024). An optimization of Blockchain parameters for improving PBFT-like finality under scale. *J. Intell. Fuzzy Syst.* 17, 501–510.

Barazanchi, I. I. A., and Hashim, W. (2023). Enhancing IoT device security through blockchain technology: a decentralized approach. *SHIFRA* 2023, 10–16. doi: 10.70470/shifra/2023/002

Basudan, S. (2023). A scalable blockchain framework for secure transactions in IoT-based dynamic applications. *IEEE Open J. Commun. Soc.* 4, 1931–1945. doi: 10.1109/OJCOMS.2022.1234567

Eghmazi, A., Ataei, M., Landry, R. J., and Chevrette, G. (2024a). Enhancing IoT data security: using the blockchain to boost data integrity and privacy. *IoT* 5, 20–34. doi: 10.3390/iot5010002

Eghmazi, A., et al., "Multi-layer architecture for scalable IoT with Hyperledger fabric and Kafka," (2024b).

El-Hajj, M., and Beune, P. (2024). Decentralized zone-based PKI: a lightweight security framework for IoT ecosystems. *Information* 15:304. doi: 10.3390/info15060304

Gong, L., Alghazzawi, D. M., and Cheng, L. (2021). BCOT sentry: a blockchain-based identity authentication framework for IoT devices. *Information* 12:203. doi: 10.3390/info12050203

Gopalan, S. H., Manikandan, A., Dharani, N. P., and Sujatha, G. (2024). Enhancing IoT security: a blockchain-based mitigation framework for deauthentication attacks. *Int. J. Networked Distrib. Comput.* 12, 237–249. doi: 10.1007/s44227-024-00029-w

Hu, V. C. (2023). NIST IR 8450 — Overview and considerations of access control based on attribute encryption. Gaithersburg, Maryland, USA: National Institute of Standards and Technology, (Final).

Janani, K., and Ramamoorthy, S. (2023). A security framework to enhance IoT device identity and data access through blockchain consensus model. *Clust. Comput.* 27, 2877–2900. doi: 10.1007/s10586-023-04113-8

Kaur, R., and Ali, A., "A novel blockchain model for securing IoT based data transmission," Int. J. Grid Distrib. Comput., vol. 14, pp. 1045–1055, (2021). Available online at: https://www.researchgate.net/publication/351437183

Kim, G., and Kim, Y. (2024). The threat of disruptive jamming to blockchain-based distributed learning in wireless networks. *Sensors* 24:535. doi: 10.3390/s24020535

Lahbib, A., Toumi, K., Laouiti, A., and Martin, S. (2024). Blockchain based distributed trust management in IoT and IIoT: a survey. *J. Supercomput.* 80, 21867–21919. doi: 10.1007/s11227-024-06286-4

Latif, S., Idrees, Z., Ahmad, J., Zheng, L., and Zou, Z. (2020). A blockchain-based architecture for secure and trustworthy operations in the industrial internet of things. *J. Ind. Inf. Integr.* 21:100190. doi: 10.1016/j.jii.2020.100190

Lee, J., Kim, M., Park, K., Noh, S., Bisht, A., Das, A. K., et al. (2023). Blockchain-based data access control and key agreement system in IoT environment. *Sensors* 23:5173. doi: 10.3390/s23115173

Liu, H., Han, D., and Li, D. (2020). Fabric-IoT: a blockchain-based access control system in IoT. *IEEE Access* 8, 18207–18218. doi: 10.1109/access.2020.2968492

Liu, B., Yao, X., Guo, K., and Zhu, P. (2023). Consortium blockchain based lightweight message authentication and auditing in smart home. *IEEE Access* 11, 68473–68485. doi: 10.1109/access.2023.3293401

Lorych, P., and Plappert, C., "Hardware trust anchor authentication for updatable IoT," ACM (2024) Attestation, measured/secure boot as off-chain mandatory controls.

Maeng, J., Heo, Y., and Joe, I. (2022). Hyperledger fabric-based lightweight group management (H-LGM) for IoT devices. *IEEE Access* 10, 56401–56409. doi: 10.1109/access.2022.3177270

Mahdavi, M., Tadayon, M. H., Haghighi, M. S., and Ahmadian, Z. (2024). IoT-friendly, pre-computed and outsourced attribute based encryption. *Futur. Gener. Comput. Syst.* 150, 115–126. doi: 10.1016/j.future.2023.08.015

Mazzocca, C., Acar, A., Uluagac, S., and Montanari, R. (2024a). EVOKE: efficient revocation of verifiable credentials in IoT networks: USENIX Security.

Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., and Conti, M. (2024b). (comprehensive overview of DIDs/VCs, threats, and adoption)). A survey on decentralized identifiers and verifiable credentials. *IEEE Commun. Surv. Tutor.* 14, 1279–1295. doi: 10.13140/RG.2.2.12726.92485

Natraj, N. A., Kishore, B., and Bhore, S. (2025). A lightweight blockchain framework for secure IoT data management: design, implementation and performance analysis. *SGS Eng. Sci.* 1.

Obaidat, M. A., et al. (2024). Exploring IoT and blockchain: a comprehensive survey on opportunities, challenges, and applications. *Information* 15.

Oktian, Y. E., Lee, S.-G., and Lee, H. J. (2020). Hierarchical multi-blockchain architecture for scalable internet of things environment. *Electronics* 9:1050. doi: 10.3390/electronics9061050

Pathak, A., Al-Anbagi, I., and Hamilton, H. J. (2023). TABI: trust-based ABAC mechanism for edge-IoT using blockchain technology. *IEEE Access* 11, 36379–36398. doi: 10.1109/access.2023.3265349

Ragul, M., Aloysius, A., and Arulkumar, V. (2025). Advancing IoT security through blockchain-driven dynamic trust evaluation. *Indian J. Sci. Technol.* 18, 526–538. doi: 10.17485/IJST/v18i7.3783

Ramezan, G., and Meamari, E., "Zk-IoT: securing the internet of things with zero-knowledge proofs on blockchain platforms," 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Dublin, Ireland, (2024a) 1–7. doi: 10.1109/ICBC59979.2024.10634342

Ramezan, G., and Meamari, E., "Zk-IoT: securing the internet of things with zero-knowledge proofs on blockchain platforms," (2024b).

Rathee, G., Ahmad, F., Jaglan, N., and Konstantinou, C. (2022). A secure and trusted mechanism for industrial IoT network using blockchain. *IEEE Trans. Industr. Inform.* 19, 1894–1902. doi: 10.1109/tii.2022.3182121

Ruzbahani, A. M.. (2024). AI-protected Blockchain-based IoT environments: harnessing the future of network security and privacy. arXiv preprint, arXiv:2405.13847.

Seshadri, S. S., Rodriguez, D., Subedi, M., Choo, K. K. R., Ahmed, S., Chen, Q., et al. (2020). IOTCOP: a Blockchain-based monitoring framework for detection and isolation of malicious devices in internet-of-things systems. *IEEE Internet Things J.* 8, 3346–3359. doi: 10.1109/jiot.2020.3022033

Shammar, E. A., Zahary, A. T., and Al-Shargabi, A. A. (2021). A survey of IoT and blockchain integration: security perspective. *IEEE Access* 9, 156114–156150. doi: 10.1109/access.2021.3129697

Shammar, E. A., Zahary, A. T., and Al-Shargabi, A. A. (2022). An attribute-based access control model for internet of things using hyperledger fabric blockchain. *Wirel. Commun. Mob. Comput.* 2022, 1–25. doi: 10.1155/2022/6926408

Singh, S., Hosen, A. S. M. S., and Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed IoT network. *IEEE Access* 9, 13938–13959. doi: 10.1109/access.2021.3051602

Tranvåg, J. B. (2025). Anchoring off-chain data to the Ethereum blockchain (with IPFS): Benchmarking and design. (MSc thesis). University of Bergen.

Vangala, A., Das, A. K., Mitra, A., Das, S. K., and Park, Y. (2022). Blockchain-enabled authenticated key agreement scheme for Mobile vehicles-assisted precision agricultural IoT networks. *IEEE Trans. Inf. Forensics Secur.* 18, 904–919. doi: 10.1109/tifs.2022.3231121

Wu, H., Liu, Y., Zhu, K., and Zhang, L. (2024). Data-sharing system with attribute-based encryption in blockchain and privacy computing. *Symmetry* 16:1550. doi: 10.3390/sym16111550

Yang, Z., Chen, X., He, Y., Liu, L., Che, Y., Wang, X., et al. (2024). An attribute-based data access control scheme using blockchain technology. *Digit Commun Netw* 4:100199. doi: 10.1016/j.hcc.2024.100199

Yang, X., Yang, X., Yi, X., Khalil, I., Zhou, X., He, D., et al. (2021). Blockchain-based secure and lightweight authentication for internet of things. *IEEE Internet Things J.* 9, 3321–3332. doi: 10.1109/jiot.2021.3098007

Yuan, F., Huang, X., Zheng, L., Wang, L., Wang, Y., Yan, X., et al. (2025). The evolution and optimization strategies of a PBFT consensus algorithm for consortium blockchains. *Information* 16:268. doi: 10.3390/info16040268

Zhao, M., Shi, C., and Yuan, Y. (2024). Blockchain-based lightweight authentication mechanisms for industrial internet of things and information systems. *Int. J. Semant. Web Inf. Syst.* 20, 1–30.

Zhou, L., Diro, A., Saini, A., Kaisar, S., and Hiep, P. C. (2024). Leveraging zero-knowledge proofs for Blockchain-based identity sharing: a survey of advancements, challenges and opportunities 80:103678. doi: 10.1016/j.jisa.2023.103678 (Example ZK identity sharing on blockchain)