Innovations in Computing and Emerging Technologies

ISSN: 3106-6518 (Print) 3106-6526 (Online) | Issue: 01
Peer-Reviewed Academic Journal

Research Article

Blockchain-Based Secure Firmware Update Mechanisms for IoT Devices- A Comprehensive Review

Kamran Mustafa[1]
Email: kamran.mustafa@uet.edu.pk

Muzaffar Ali Khan [1]
Email:muzaffar.khanji@outlook.com

Muhammad Hamza Farooq [2]
Email: hamza.farooq@umt.edu.pk

Ashir Kamal[1]
Email: ashir.kamal@uet.edu.pk

Submitted	Accepted	Published	Article No.
4-Nov-25	28-Nov-25	19-Dec-25	ICET0125-275

Affiliations:
[1] *Department of Computer Science, University of Engineering and Technology Lahore, Pakistan.*
[2] *Department of Informatics and Systems, University of Management Technology Lahore.*

Abstract

The rapid increase in Internet of Things (IoT) devices, expected to reach 29 billion by 2030, has brought firmware security into the spotlight. The traditional mechanisms for updating devices rely on central entities, which are prone to single points of failure, integrity violations, and scalability constraints. Blockchain technology ensures decentralized mechanisms for protected records, cryptographic defense and clear auditability. This paper performs a systematic review of 36 peer-reviewed studies published between 2017 and 2025 that address blockchain-based secure firmware update mechanisms for IoT devices. Proposed architectures, agreed protocols, security attributes and performance indicators were analyzed and classified by blockchain platforms such as Ethereum, Hyperledger Fabric and IOTA storage approaches like IPFS and distributed systems authentication techniques, including PUF-based and smart contract-based methods and deployment scenarios represented by LoRaWAN, UAV-assisted and industrial IoT. The review demonstrates high levels of decentralized verification, an immutable audit trail and automation through smart contracts. However, there are still critical issues that remain unresolved, including the inability of solutions currently available to scale to 100,000 devices and more, a power overhead of 8 -15 percent caused by blockchain activity, lack of cross-platform interoperability, and insufficient analysis of the security vulnerabilities of smart-contracts. Future studies ought to anticipate Layer-2 scaling approaches, energy-efficient cryptography primitives, standardization, and hybrid architecture designs so that the practice of using blockchain-based firmware security in heterogeneous IoT settings can be realized in practice.

Keywords: Blockchain, Internet of Things (IoT), Firmware Updates, Security, Decentralization, Scalability, Consensus Mechanisms

1 Introduction

Internet of Things (IoT) has permeated into the modern infrastructure, cutting across such transformative industries as healthcare, industrial automation, smart cities, precision agriculture, as well as transportation [20]. The number of connected devices is projected to increase to approximately 29 billion by 2030, compared to 25 billion in 2020 [29], and hence it is a significant improvement [37]. Although this proliferation has enabled major steps forward in efficiency, safety and user experience, it is also introducing serious security threats, especially in the underlying layer of device behaviour control, that is, firmware management [19].

Software applications can easily be corrected, whereas firmware vulnerabilities are hard to fix at scale and thus significantly more dangerous. Firmware updates are also mandatory, and secure timely update of firmware is therefore essential [4]. They reduce the vulnerabilities, ensure that the devices are compatible with new standards and hedge against threats that are being discovered [13]. However, some researchers found that most of the security incidents involving IoT are due to the unpatched firmware vulnerabilities despite the existence of patches [12]. In the Verizon Data Breach Investigations Report, it can be stated that one-third of organizational break-ins are related to IoT devices [36], which reflects systemic shortcomings in current update architectures.

Traditional over-the-air (OTA) update systems, which are centralized in nature, contribute to those challenges [5]. They are prone to single points of failure, weak integrity checks, minimal transparency, as well as bottlenecks in scaling [35]. Such vulnerabilities are also aggravated by the resource-constrained characteristic of the IoT devices [23], which do not usually have enough computational power, memory, and energy budgets to support a strong security posture [6]. All these are contributing elements that have created an existing menace to IoT ecosystems. The technology of blockchain suggests a paradigm shift. It has a decentralized trust structure, audit trails that are immutable, cryptography guarantees, and automation through smart contracts, all of which deal with many of the shortcomings of centralized systems [15]. With blockchain, it is possible to verify with transparency, which allows the independent audit of the provenance of the firmware and the integrity of the supply chain (e.g. Fig. 1). The industry trend agrees with this vision- the blockchain-IoT market will grow with a compound annual growth rate (CAGR) of 58.21 -1, starting with USD 761.03 million in 2024 and reaching USD 74,772.36 million in 2034 [37].

Nevertheless, studies are incomplete despite this promise. Various strategies on platforms, consensus, storage models and authentication techniques leave the key question unanswered, such as scalability, energy efficiency, cross-platform and standardization [22]. These are the gaps that should be filled in to shift the usage of blockchain-based firmware security from prototypical to a production-ready system [17].

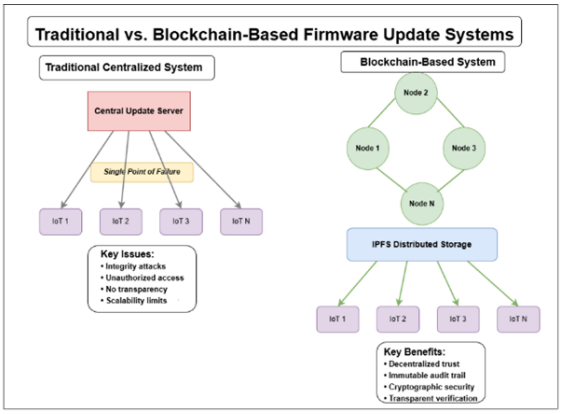

Figure 1: Comparison between traditional centralized and blockchain-based firmware update systems.

The contribution of this paper to the field is to synthesize 36 peer-reviewed articles published in the past 2017-2025, make comparative studies across platforms, mechanisms, and architectures and discover gaps that need to be addressed. It provides a viable advice to researchers, practitioners and policymakers seeking to provide secure, scalable and transparent firmware updates to the billions of Internet of Things devices that form the backbone of the contemporary digital infrastructures.

2 Literature Review

Until 2017, there was pressure to solve the impending vulnerabilities associated with centralized mechanisms for updating firmware in IoT devices. Therefore, this section provides a review of existing research in a thematically categorized manner, representing various architectural approaches and areas of technological focus. A comparative summary is provided in Table 1. In each category, specific challenges in the field of IoT firmware security are being met while availing the fundamental properties of blockchain- decentralization, immutability, and cryptographic verification.

2.1 Decentralized Storage-Based Firmware Update Models

Various works combine blockchain with a decentralized storage system to avoid the single point of failure related to firmware distribution. Lin and Bo [1] were among the first to present the integration of IOTA Streams with IPFS for industrial IoT, ensuring integrity via cryptographic hashing but presenting issues with latency in pull-based models. Sabarishraj et al. [2] furthered this work by providing an implementable FOTA system with hybrid AES–ECC encryption and compression, conceptualizing UAV-based delivery for disconnected devices. Biro et al. [3] further proposed gateway-mediated dispatch, which reduces device-side computation at the cost of dependency on gateways. Mtetwa et al. [31] combined Ethereum smart contracts with IPFS, finding a balance between security and efficiency but pointing out the issue of gas costs. Son et al. [23] further improved this with a broker-based architecture on Hyperledger Fabric, achieving scalability and sub-second verification latency.

2.2 Blockchain Platform-Specific Firmware Update Systems

2.2.1 Ethereum-Based Mechanisms

Ethereum smart contract ecosystem adoption has been large. Sey et al. [8] proposed Firmblock, which leverages IPFS with associated revocation mechanisms to mitigate malware and compromised keys, but suffers from high energy costs. Akkaoui et al. [7] proposed the use of PUF-based authentication in medical IoT, which ensures device identity with significant economic barriers. Yohan and Lo [25][28][33] proposed the FOTB framework, which supports both PUSH-PULL updates and comes with formal security analysis at the expense of a throughput being limited for large-scale deployments. Gupta [26] stressed the need for consumer IoT resilience by managing firmware hashes over Ethereum, but at the cost of blockchain client capabilities. Tsaur et al. [27] proposed an architecture with multi-stage validation, which enhances the security but at increased complexity.

2.2.2 Hyperledger-Based Solutions

Hyperledger Fabric's permissioned architecture fits enterprise IoT. Ahn et al. [9] designed onboard security modules for smart inverters, ensuring almost full malware detection. Sanchez-Gomez et al. [10] contributed the integration of LoRaWAN and OSCORE, SCHC compression, IPFS, and Hyperledger, with a high success rate in smart agriculture deployments. He et al. [21] proposed a compiler that generates chain codes automatically, with fewer errors, and faster adaptation can be made. He et al. [32] realized OTA updates on Hyperledger; while these update methods mitigate attacks, they increase latency and energy consumption. Seo et al. [30] pioneered a distribution assisted by UAVs, showing feasibility but at high operational costs.

2.2.3 IOTA and Alternative Platforms

IOTA's Tangle allows for feeless transactions and is scalable. Lin and Bo [1] utilized IOTA Streams for light-weight updates, but the maturity of the ecosystem is low. Yohan et al. [18] used technology initially based on a skip chain that reduced the complexity and

resource consumption in the verification process. Expanding their former work, Yohan et al. [25] proposed a robust framework with a dual-link verification mechanism and secure life cycle protocols. Their system decreases computational overhead by 40 – 60%, still being able to maintain equivalent security guarantees, which has been validated on ESP8266 and Raspberry Pi devices. Scalability was, however, not tested above 5,000 devices, leaving open questions for large-scale IoT deployments.

2.3 Authentication-Enhanced Firmware Update Models

Mechanisms for authentication ensure that updates reach only legitimate devices. Joshi et al. proposed PUF-based frameworks that register immutable device identities on blockchain, but this also has a number of requirements regarding error correction because of aging effects. Islam and Kundu extended PUF integration on feature management in ICs by allowing secure ownership transfer and reducing manufacturing costs. Akkaoui [7] applied PUF authentication to medical IoT to ensure conformity with the established regulatory standards. Ansay et al. [16] proposed Gnomon, a decentralized identifier and verifiable credentials-based solution for 5G IoT, which achieved massive scalability with minimal overhead.

2.4 Lightweight, LoRaWAN, and LPWAN-Optimized Models

Resource-constrained IoT devices are in need of tailored solutions. Mtetwa et al. [12][31] designed LoRaWAN-compatible blockchain updates, achieving 87% success in agricultural deployments but requiring multi-day update windows. Fukuda and Omote [11] introduced incentive models where the manufacturers give rewards to distributors while reducing device-side costs. Anastasiou et al. [34] addressed packet loss with redundancy and error correction, requiring multiple gateways for reliability. Sanchez-Gomez et al. [10] showed SCHC compression, reducing overhead by up to 85%. Table **??**

2.5 UAV-Assisted and Hybrid Firmware Distribution

UAVs allow updates in disconnected environments. Sabarishraj et al. [2] envisioned the UAV delivery, whereas most issues still remain practical. Biro et al. [3] referred to UAV-based extensions for gateway mediated systems. Seo et al. [30] implemented UAV-assisted distribution on Hyperledger. It achieved high success rates but was economically constrained. Yohan and Lo [28] proposed hybrid PUSH–PULL architectures adapted to UAV, satellite, or mesh networks.

2.5.1 Identity Management and Decentralized Credentials

At the heart of secure updates are robust mechanisms of identity management. Ansay et al. [16] designed the Gnomon for decentralized identity in 5G IoT, avoiding reliance on centralized certificate authorities. Natraj et al. [24] conducted a critical analysis of incorporating blockchain technology in the Internet of Things (IoT), with the prominent differences between the academic prototypes and practical applications. Their methodical review of 49 studies indicated that there could be no scalability beyond the controlled testbed settings and that no report could support more than 100,000 devices, despite the millions of devices normally deployed within the industrial IoT setting. The authors were able to identify three common architectures, which include Ethereum-based smart contracts, Hyperledger Fabric and hybrid blockchain-IPFS systems, each with a different limitation based on cost, latency or the complexity of implementation. Energy overhead comparisons with centralized ones showed increments of between 8 to 15, which is a formidable obstacle to battery-operated equipment. The research also condemned the current disintegration and incompatibility of the available solutions and proposed the creation of a full suite of benchmarks, interoperable models, and integration with the existing platforms of the IoT. The analysis highlights the necessity to shift the use of proof-of-concept prototypes into scalable, standardized, and sustainable blockchain-based security solutions for IoT firmware.

2.6 Supply Chain Security and SBOM Integration

Firmware security can be extended to supply chain integrity. Anonymous 2019 proposed the integration of SBOM with blockchain, which allows for provenance verification while facing overhead in SBOM generation. Tinnaluri et al. [6] show trust-based access control to reduce malware propagation. Choi et al. [14] address manufacturer disappearance by extending SUIT with blockchain and IPFS, allowing multi-party governance, and long-term utility of devices.

3 Methodology

It focuses on the identification, analysis, and synthesis of research on blockchain-based secure firmware update mechanisms of IoT devices. In conducting the systematic review, 36 peer-reviewed publications between 2017 and 2025 were identified using structured database searching combined with multi-stage screening (e.g. Fig. 2). The review addresses four research questions that look at blockchain frameworks, platform effectiveness, security mechanisms, and implementation challenges in IoT firmware security.

Table 1: Comparison of Blockchain-based OTA Update Systems for IoT

Ref	Platform / Method	Key Innovation	Strengths	Limitations	Best Application
[1]	IOTA + IPFS	Feeless transactions, pull-based updates	Lightweight, resilient	Latency in pull models	Industrial IoT
[2]	IPFS + UAV Concept	Hybrid AES+ECC, compression	Efficient for constrained devices	UAV delivery theoretical	Remote IoT
[3]	Ethereum + IPFS	Gateway-mediated dispatch	Reduced device load	Gateway dependency	Gateway IoT
[18]	Ethereum + IPFS	Revocation system	Malware resilience	High energy cost	General IoT
[7]	Ethereum + PUF	Medical IoT authentication	Hardware-rooted security	Economic barriers	Healthcare IoT
[25][28][33]	Ethereum FOTB	PUSH–PULL dual mechanism	Formal security analysis	Limited throughput	Large IoT networks
[26]	Ethereum + IPFS	Decentralized OTA	Independent of the manufacturer	Requires a blockchain client	Consumer IoT
[27]	Ethereum	Defense-in-depth validation	Strong security	Complexity overhead	Secure IoT
[9]	Hyperledger	Onboard security module	98.7% malware detection	Limited scope	Renewable energy IoT
[10]	Hyperledger + LoRaWAN	SCHC compression	High success rate	Infrastructure cost	Smart agriculture
[21]	Hyperledger DSL	Automatic chaincode generation	Reduced errors	DSL learning curve	Enterprise IoT
[32]	Hyperledger OTA	Distributed OTA	Fault tolerance	Higher latency	Commodity IoT
[30]	Hyperledger + UAV	UAV-assisted delivery	Remote coverage	High operational cost	Disaster recovery
[18]	Skip chain (early)	Efficient verification	Reduced complexity	Limited adoption	Constrained devices

3.1 Objectives and Scope

The main objective is a critical review of secure firmware update mechanisms in IoT devices built on blockchain technology. Therefore, solutions are envisaged that apply blockchain for secure, verifiable, and scalable firmware delivery across heterogeneous IoT ecosystems. The review aims to- Identify & classify the existing frameworks and approaches for secure firmware updates. Comparing blockchain platforms used for firmware update - Ethereum, Hyperledger and IOTA. Analyze security enhancements and limitations of proposed solutions. Identify research gaps and propose future directions in blockchain-based firmware update mechanisms.

3.2 Research Questions

The research questions addressed in this study are as follows-

1. RQ1- What are the existing blockchain-based frameworks and models proposed for secure firmware updates in IoT environments?
2. RQ2- How do various blockchain technologies (e.g., Ethereum, Hyperledger, IOTA) impact the effectiveness and performance of secure firmware updates?
3. RQ3- What are the common security enhancements and limitations of existing blockchain-based firmware update mechanisms for IoT devices?
4. RQ4- What are the critical research gaps and challenges in adopting blockchain for secure and scalable firmware updates in real-world IoT deployments?

3.3 Search Strategy and Data Sources

A thorough literature review was conducted in several academic databases to cover all peer-reviewed publications on blockchain-based IoT firmware security exhaustively. The search strategy involved systematic database searches and forward and backward citation searches to help determine the major contributions to the field, as well as the recent ones.

3.4 Databases Searched

The systematically contacted academic databases and online libraries included the following

- IEEE Xplore Digital Library - The main source of conference papers, IEEE journals and publications on blockchain, IoT security and embedded systems.

- SpringerLink - To access journal articles and conference proceedings in the fields of computer science and security.
- ScienceDirect (Elsevier) - To access premium journals such as sensors, electronics and security-related materials.
- Google Scholar - This is used to cover all the areas, track citations, and to find cross-disciplinary research.
- arXiv.org – Preprints and developing research in computer science, especially new developments.

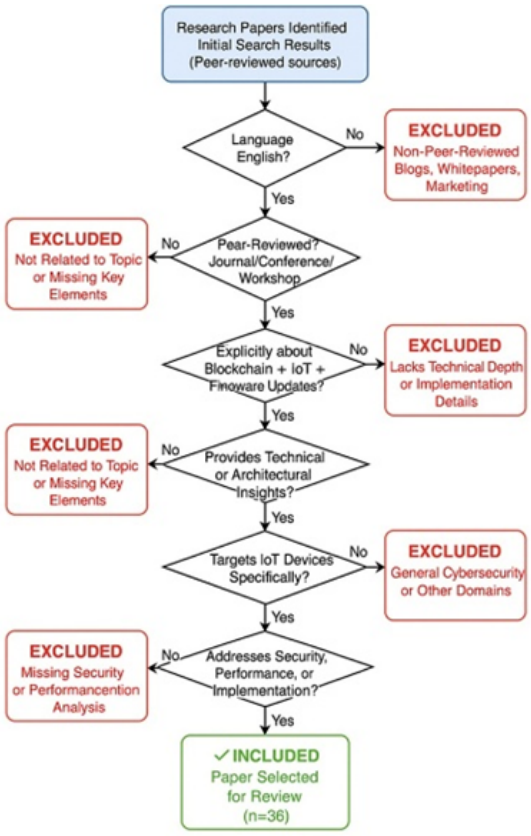

Figure 2: Systematic Literature Review Screening Process Multi-stage filtering process from 361 initial papers through deduplication (298), title or abstract screening (82) and full-text assessment, yielding 36 papers meeting all inclusion criteria and quality standards for comprehensive analysis.

3.5 Search Terms

The search query was a Boolean query that was systematically used in all academic databases-(blockchain OR Ethereum OR Hyperledger) AND (firmware update) AND (IoT or Internet of Things). Refinements based on the databases were used where necessary, such as subject filters of Security, Blockchain Technology, Internet of Things, and Embedded Systems, to ensure better accuracy of retrieval.

3.6 Search Period January 2017 to August 2025

The search of the systematic database provided the list of 361 papers in all sources before the screening criteria were applied.

The temporal coverage of eight years was chosen because it will help understand the transformation of blockchain and IoT integration studies in theory (2017 to 2019) to their application and deployment (2025). The year 2017 is the beginning of the mature blockchain platforms that can be used to integrate the IoT, and August 2025 is a guarantee of incorporating the latest improvements.

3.7 Inclusion and Exclusion Criteria.

In order to have a systematic and rigorous selection of papers, clear criteria were laid down to be able to ascertain qualification to be included in this review. Table 2 shows the full inclusion and exclusion criteria used in the process of multi-stage screening.

3.8 Paper Selection and Screening Process

Paper selection was done through a multi-step process based on best practices for the systematic literature review. On each step, it applied more and more refined selection criteria in order to include publications of the highest quality that matched the relevance criteria.

1. Step 1- Initial Search and Deduplication
   Total papers identified across all databases: 361 Duplicates removed-different databases indexed same paper: 63 Papers left after deduplication: 298
2. Stage 2: Title and Abstract Screening
   All 298 papers underwent initial relevance screening based on title and abstract content. Papers were excluded at this stage if they clearly fell outside the scope of the review.
   - Excluded non-IoT blockchain applications. General Distributed Systems, Cryptocurrency, Supply Chain without Firmware Context: 127 papers
   - Excluded- Non-firmware security topics - data integrity, communication protocols, access control without update mechanisms: 89
   - papers Papers advancing to full-text review: 82
3. Stage 3- Full-Text Assessment
   A total of 82 remaining papers were evaluated in detail against all the inclusion criteria and research questions through full-text assessment. Exclusions were based on:

Table 2: Inclusion and Exclusion Criteria Applied in the Systematic Literature R

Inclusion Criteria	Exclusion Criteria
Peer-reviewed journal articles, conference papers, and workshop proceedings from established academic venues	Non-peer-reviewed articles, blogs, whitepapers, marketing materials, technical reports, dissertations, and book chapters
Papers explicitly proposing, evaluating, or discussing blockchain-based solutions for firmware updates in IoT devices	Papers focusing on blockchain applications unrelated to firmware updates (e.g., supply chain traceability only, cryptocurrency, data sharing platforms)
Papers providing technical and/or architectural insights into blockchain frameworks, implementation details, performance evaluation, or security analysis	Papers lacking technical depth, purely conceptual without implementation insights, or insufficient architectural description
Papers specifically targeting IoT devices, embedded systems, sensor networks, edge computing, or industrial IoT environments	Papers not explicitly addressing IoT devices; general cybersecurity papers without an IoT context; enterprise or cloud-only software updates
Papers addressing security mechanisms, performance metrics, scalability evaluation, or implementation challenges in firmware update processes	Papers lacking any security analysis, performance evaluation, experimental validation, or practical implementation considerations
English language publications to ensure consistent analysis and interpretation	Non-English language publications are due to resource constraints in translation and verification
Papers published between January 2017 and January 2025 to capture recent developments and the current state-of-the-art	Papers published before 2017 to focus on modern blockchain platforms and contemporary IoT security challenges
Papers contributing substantive insights to at least one of the four research questions (RQ1-RQ4) with clear methodological or technical contributions	Papers tangentially mentioning blockchain or IoT without substantive contribution to firmware update security, or lacking clear research contributions

- Insufficient technical depth or architectural details: 28 papers
- Lack of performance evaluation, security analysis, or implementation validation: 11 papers
- General surveys or position papers without specific technical contributions: 7 papers
- Final papers included in systematic review: 36

4. Screening Validation
   The lead researcher conducted the primary screening of titles and abstracts. In cases of uncertainty or doubt, verification of such borderline cases was sought through consultation with domain experts. Full-text review followed a detailed evaluation against all four research questions and the quality assessment criteria. Forward and backward citation tracking on seminal papers identified during the review process was completed to ensure comprehensiveness, leading to the identification of three additional papers that were included after meeting all criteria.

3.9 Data Extraction and Analysis

A systematic framework for data extraction was developed to compare data from 36 papers. Information gathered included metadata on publication, blockchain architecture (Ethereum, Hyperledger, and IOTA), consensus mechanisms (PoW, PoS, PBFT, and Tangle), storage models (on-chain, off-chain via IPFS, hybrid), and methods of performing firmware update (PUSH, PULL, hybrid). Authentication approaches were varied from Physical Unclonable Functions and PKI through to smart contracts and hardware security modules.

Performance metrics- latency, throughput, energy use, bandwidth, computational overhead, scalability. Security analysis of integrity verification (hashes, Merkle trees), signatures, authentication, access control, attack resistance, and formal security proofs. Implementation contexts- device types, deployment scenarios (agriculture, healthcare, industrial IoT, smart cities), evaluation methods (testbeds, simulations), and limitations (scalability, cost, integration).

The data was standardized for consistency and thematically analyzed across seven research trajectories-decentralized storage, platform-specific solutions, authentication-enhanced models, lightweight LoRaWAN designs, UAV-assisted distribution, supply chain security, and identity management. Comparative analysis searched for trade-offs in the dimensions of security, performance, scalability, resource efficiency, and deployment suitability. Gaps identified included overstated scalability, limited real-world validation, lack of quantum-resistant cryptography, poor key management, and minimal discussion on regulatory compliance (e.g. Table 3). Mapping to research questions showed strong coverage of frameworks (RQ1), moderate comparative performance analysis (RQ2), extensive but uneven security evaluation (RQ3) and limited discussion of real-world challenges (RQ4). These findings point toward several directions for future efforts- interoperability, sustainability, and practical deployment of blockchain-based IoT firmware security.

Table 3: Coverage Analysis of Research Questions by Category

Category	RQ1	RQ2	RQ3	RQ4	Count
Decentralized Storage Models	✓	✓	✓	✓	5
Ethereum-Based Approaches	✓	✓	✓	✓	7
Hyperledger-Based Approaches	✓	✓	✓	✓	5
Authentication-Enhanced Models	✓	o	✓	✓	4
LPWAN / LoRaWAN-Optimized Models	✓	✓	✓	✓	5
UAV-Assisted / Hybrid Delivery	✓	o	o	✓	3
Supply Chain & SBOM-Based Solutions	✓	o	✓	✓	3
Identity / Decentralized Credentials	✓	o	✓	o	3
Critical Review / Survey Papers	o	o	✓	✓	1
Total Coverage	**1**	**0.78**	**0.94**	**0.86**	

4 Results and Discussion

The systematic review of 36 studies reveals six dominant architectural approaches shaping blockchain-based secure firmware update mechanisms for IoT systems. Decentralized storage-driven models, which combine blockchain with off-chain repositories such as IPFS, improve firmware integrity and provenance at the cost of latency, availability constraints and gateway dependency. Platform-specific frameworks demonstrate well-differentiated performance and trust characteristics- Ethereum offers rich programmability while commanding high transaction costs and unpredictable latency; Hyperledger Fabric offers deterministic performance well-suited to enterprise contexts; and IOTA enables lightweight, feeless transactions without large-scale empirical validation. Smart contract–based architectures automate authorization, versioning and policy enforcement, helping to enhance transparency and mitigate rollbacks, while introducing systemic risks due to the immutability of contracts, coding vulnerabilities and execution overhead. Hardware-assisted authentication approaches, including PUFs provide strong device identity assurance and key compromise resistance, though their hardware costs and environmental sensitivities limit applicability in large-scale or low-cost deployments. Lightweight LPWAN-oriented models, conceived for LoRaWAN and similar networks, use compression and fragmentation to enable updates under extremely tight bandwidth constraints; this, however, comes at the expense of prolonged update duration due to low throughput, limiting practicality for large firmware images. UAV-assisted and hybrid delivery mechanisms increase the reach to remote or intermittently connected settings by using blockchain verification of firmware alongside mobile or aerial distribution, and meanwhile result in high operational costs and increased physical and communication-layer security risks. Overall, findings derived here indicate that, although blockchain contributes significantly to the integrity, transparency, and trust of firmware delivery, no single architectural family satisfies the combined requirements of scalability, energy efficiency, cost-effectiveness, and real-world deployability across diverse IoT environments. Rather, each of these approaches embodies particular trade-offs, suggesting that hybrid, context-aware designs will be required to achieve robust and scalable blockchain-enabled firmware update ecosystems.

5 Research Gaps and Limitations

Although significant progress has been made towards blockchain-based firmware update systems for Internet of Things (IoT) systems, there are still several critical research gaps. First of all, the biggest limitation includes scalability. None of the suggested frameworks show consistent performance even in moderately-sized deployments, and none of them has proven blockchain-assisted updates at the scale of millions of devices, which is a common requirement of an industrial IoT system. Second, the problem of energy limits in resource-limited devices is poorly handled. The existing solutions impose an energy overhead of 8-15% because of cryptography verification and blockchain communication, and they cannot be used in battery-powered or long-life-cycle IoT devices.

Third, interoperability and standardization are greatly lacking in the literature. The vast majority of frameworks are closely linked to a particular blockchain platform, communication protocol or hardware setup, thus restricting inter-vendor interoperability and maintainability.

Fourth, the security of smart contracts is a risk that is under-researched. Even though smart contracts are usually part of core verification, little research uses formal verification, auditing processes, or secure design practices, so update processes can be exploited by contract-level attacks.

Fifth, there is a lack of support for the unique needs of offline or intermittently connected IoT devices. The mechanisms of UAV-assisted or pull-based solutions to the problem address only partial sides of the issue and lack comprehensive consideration of secure synchronization, conflict-free state management, or distributed trust bootstrapping.

Lastly, the existing systems do not have dynamic trust management features. They also usually presuppose non-dynamical identities and trust relationships, which are far off-model to real-world IoT networks with device churn, changes in owners and threats, and dynamical threat landscapes. These gaps will be necessary to fill in to create secure, scalable and practical blockchain-based firmware update ecosystems.

6 Conclusions and Future Work

This systematic review presented 36 peer-reviewed studies on blockchain-based secure firmware update mechanisms for IoT devices, indicating remarkable progress in decentralizing verification and offering immutable provenance tracking as well as automated update authorization. Blockchain demonstrably strengthens firmware integrity, mitigates rollback, tampering attacks and increases transparency for multi-stakeholder IoT ecosystems. However, it also follows from the findings that no current architecture fully meets the combined requirements of scalability, energy efficiency, interoperability, and deployment feasibility within heterogeneous IoT contexts. Most proposals remain limited to computational overhead, communication limitations, and platform-specific dependencies, while large-scale, real-world validations are noticeably missing.

Some promising research directions are foreseen in the near future. The focus of future research shall be on lightweight and scalable blockchain architectures, including Layer-2 solutions, DAG-based ledgers, and sharding techniques, which can support millions of IoT nodes. Second, energy-efficient cryptographic primitives and verification protocols will be necessary to reduce the burden for constrained devices. Interoperability frameworks and standardized interfaces, such as IETF SUIT and W3C DID, should be designed to guarantee cross-vendor compatibility and long-term maintainability. Moreover, secure and formally verified smart contracts have to be devised that avoid vulnerabilities in the update authorization logics. For settings that are remote or intermittently connected, hybrid dissemination models, including UAV- and mesh-assisted dissemination, need to be developed with enhanced synchronization and trust-bootstrapping mechanisms. Finally, the integration of AI-driven anomaly detection, adaptive trust management and post-quantum security techniques can offer substantial resilience against emerging threats. This positions the future research directions to continue improving blockchain-enabled firmware update systems toward robust, scalable and globally deployable solutions that will meet the demands of the rapidly growing IoT landscape.

References

[1] Iuon-Chang Lin and Ling Bo, "A Pull Firmware Update Mechanism for Industrial Control Based on IOTA Streams," 2024 19th Asia Joint Conference on Information Security (AsiaJCIS), IEEE, 2024.

[2] Sabarishraj K., Jayanthy S., Judeson Antony Kovilpillai J., Sabari Santhosh S., and Swathi R., "Efficient Implementation of Firmware Over-the-Air Update using Raspberry Pi 4 and STM32F103C8T6," 2024 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), IEEE, 2024.

[3] Vince Biro, Wei-Yang Chiu, and Weizhi Meng, "Securing IoT Firmware Dispatch Systems with Blockchain," 2023 IEEE International Conference on Blockchain (Blockchain), IEEE, 2023.

[4] Himanshu Joshi, Anshu S Anand, and J Kokila, "Secure Firmware Update Architecture for IoT Devices using Blockchain and PUF," 2023 IEEE International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (iQ-CCHESS), IEEE, 2023.

[5] Anonymous, "A Secure Firmware and Software Update Model Based on Blockchains for Internet of Things Devices Using SBOM," 2023 18th Asia Joint Conference on Information Security (AsiaJCIS), IEEE, 2023.

[6] V. S. Narayana Tinnaluri, A. Jyothi Babu, P. Shanmugaraja, S. Satheesh Kumar, and A. Pai H., "A Productive Model for Secured Data Sharing in Blockchain Technology based IoT," Proceedings of the International Conference on Inventive Computation Technologies (ICICT 2023), IEEE, 2023.

[7] R. Akkaoui, "Blockchain for the Management of Internet of Things Devices in the Medical Industry," IEEE Transactions on Engineering Management, vol. 70, no. 8, pp. 2707-2717, 2023.

[8] C. Sey, H. Lei, W. Qian, X. Li, L. D. Fiasam, R. Sha, and Z. He, "Firmblock: A Scalable Blockchain-Based Malware-Proof Firmware Update Architecture with Revocation for IoT Devices," Proceedings of the 18th International Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), IEEE, 2021.

[9] B. Ahn, J. Choi, G. Bere, T. Kim, S. Ahmad, and S.-w. Park, "Blockchain-Enabled Security Module for Transforming Conventional Inverters toward Firmware Security-Enhanced Smart Inverters," Proceedings of the 2021 IEEE Energy Con-

version Congress and Exposition (ECCE), IEEE, 2021.

[10] J. Sanchez-Gomez, R. Marin-Perez, M. Ross, and A. F. Skarmeta Gomez, "Holistic IoT Architecture for Secure Lightweight Communication, Firmware Update, and Trust Monitoring," Proceedings of the 2021 IEEE International Conference on Smart Internet of Things (Smart-IoT), IEEE, 2021.

[11] T. Fukuda and K. Omote, "Efficient Blockchain-based IoT Firmware Update Considering Distribution Incentives," IEEE Conference on Dependable and Secure Computing (DSC), 2021.

[12] N. S. Mtetwa, N. Sibeko, P. Tarwireyi, and A. M. Abu-Mahfouz, "OTA Firmware Updates for LoRaWAN Using Blockchain," Proceedings of the 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC), IEEE, 2020.

[13] J. L. Hernandez-Ramos, G. Baldini, S. N. Matheu, and A. Skarmeta, "Updating IoT Devices: Challenges and Potential Approaches," Proceedings of the 2020 IEEE International Conference on Standards for Communications and Networking (CSCN), IEEE, 2020.

[14] S. Choi and J.-H. Lee, "Blockchain-Based Distributed Firmware Update Architecture for IoT Devices," IEEE Access, vol. 8, pp. 37518-37534, 2020.

[15] C. Gao, L. Luo, Y. Zhang, B. Pearson, and X. Fu, "Microcontroller Based IoT System Firmware Security: Case Studies," Proceedings of the 2019 IEEE International Conference on Industrial Internet (ICII), IEEE, 2019.

[16] R. Ansay, J. Kempf, O. Berzin, C. Xi, and I. Sheikh, "Gnomon: Decentralized Identifiers for Securing 5G IoT Device Registration and Software Update," 2019 IEEE International Conference on Communications Workshops (ICC Workshops), IEEE, 2019.

[17] N. Mtetwa, P. Tarwireyi, and M. Adigun, "Secure the Internet of Things Software Updates with Ethereum Blockchain," Proceedings of the 2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), IEEE, 2019.

[18] A. Yohan, N.-W. Lo, and L. P. Santoso, "Secure and Lightweight Firmware Update Framework for IoT Environment," Proceedings of the 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE), IEEE, 2019.

[19] M. N. Islam and S. Kundu, "Remote Configuration of Integrated Circuit Features and Firmware Management via Smart Contract," 2019 IEEE International Conference on Blockchain (Blockchain), IEEE, 2019.

[20] E. N. Witanto, Y. E. Oktian, S. Kumi, and S.-G. Lee, "Blockchain-based OCF Firmware Update," Proceedings of the 2019 International Conference on ICT Convergence (ICTC), IEEE, 2019.

[21] X. He, R. Gamble, and M. Papa, "A Smart Contract Grammar to Protect IoT Firmware Updates Using Hyperledger Fabric," Proceedings of the 2019 IEEE International Conference on Omnilayer Intelligent Systems (COINS), IEEE, 2019.

[22] A. Pillai, S. M, and L. K. V, "Securing Firmware in Internet of Things Using Blockchain," Proceedings of the 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), IEEE, 2019.

[23] M. Son and H. Kim, "Blockchain-Based Secure Firmware Management System in IoT Environment," Proceedings of the 2019 International Conference on Advanced Communications Technology (ICACT), IEEE, 2019.

[24] N. A. Natraj, J. J. Midhunchakkaravarthy, and B. K. Mishra, A quantitative framework for the selection of hybrid consensus mechanisms in Blockchain-IoT systems, EAI Endorsed Transactions on Internet of Things, vol. 11, Nov. 2025. doi: 10.4108/eetiot.10249.

[25] A. Yohan and N.-W. Lo, "An Over-the-Blockchain Firmware Update Framework for IoT Devices," Proceedings of the 2018 IEEE 4th International Conference on Big Data Security on Cloud (Bigdata Security), IEEE, 2018.

[26] P. Gupta, "A Decentralized Approach Towards Secure Firmware Updates and Testing Over Commercial IoT Devices," arXiv preprint arXiv:2011.12052, 2020.

[27] W.-J. Tsaur, J.-C. Chang, and C.-L. Chen, "A Highly Secure IoT Firmware Update Mechanism Using Blockchain," Sensors, vol. 22, no. 2, p. 530, 2022.

[28] A. Yohan and N.-W. Lo, "An Over-the-Blockchain Firmware Update Framework for IoT Devices," Proceedings of the 2018 IEEE Conference on Dependable and Secure Computing (DSC), IEEE, 2018.

[29] B. Lee and J.-H. Lee, "Blockchain-Based Secure Firmware Update for Embedded Devices in an Internet of Things Environment," The Journal of Supercomputing, vol. 73, no. 3, pp. 1152-1167, 2017.

[30] J. W. Seo, A. Islam, M. Masuduzzaman, and S. Y. Shin, "Blockchain-Based Secure Firmware Update Using an UAV," Electronics, vol. 12, no. 10, p. 2189, 2023.

[31] N. S. Mtetwa, P. Tarwireyi, C. N. Sibeko, A. Abu-Mahfouz, and M. Adigun, "Blockchain-Based Security Model for LoRaWAN Firmware Updates," Journal of Sensor and Actuator Networks, vol. 11, no. 5, 2022.

[32] X. He, S. Alqahtani, R. Gamble, and M. Papa, "Securing Over-The-Air IoT Firmware Updates using Blockchain," Proceedings of the International Conference on Omni-layer Intelligent Systems (COINS), 2019.

[33] A. Yohan and N.-W. Lo, "FOTB: A Secure Blockchain-Based Firmware Update Framework for IoT Environment," International Journal of Information Security, vol. 19, pp. 257-278, 2020.

[34] A. Anastasiou, P. Christodoulou, K. Christodoulou, V. Vassiliou, and Z. Zinonos, "IoT Device Firmware Update over LoRa: The Blockchain Solution," Proceedings of the 2020 International Conference on Distributed Computing in Sensor Systems (DCOSS), IEEE, 2020.

[35] J. L. Hernandez-Ramos, G. Baldini, S. N. Matheu, and A. Skarmeta, "Updating IoT Devices: Challenges and Potential Approaches," Proceedings of the 2020 IEEE International Conference on Internet of Things (iThings), 2020.

[36] Verizon, "2024 Data Breach Investigations Report," 2024. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/. [Accessed: Oct. 2025].

[37] Precedence Research, "Blockchain IoT Market Size, Share, and Trends 2025 to 2034," Jan. 2025. [Online]. Available: https://www.precedenceresearch.com/blockchain-iot-market. [Accessed: Oct. 2025].