Innovations in Computing and Emerging Technologies

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

K Mustafa [1,2], M. H. Farooq [1], M. A. Khan [1] and A. Kamal [1]

[1] Dept. of Computer science, University of Engineering & Technology (UET), Lahore, kamran.mustafa@uet.edu.pk
[2] Dept. of Informatics and Systems UMT Lahore. hamza.farooq@umt.edu.pk
[3] Dept. of Computer Science, University of Engineering and Technology, Lahore, 2023mscs23@student.uet.edu.pk
[4] Dept. of Computer Science, University of Engineering and Technology, Lahore, ashir. kamal@.uet.edu.pk

Received on 08 Nov 2025: Revised on 24, Nov 2025 Accepted: 2025

Abstract - Over the years, the Internet of Things (IoT) has been growing exponentially, which resulted in the massive use of connected devices in different fields, such as healthcare, industrial systems, smart cities and critical infrastructure. To protect the security, functionality and efficiency of these devices, firmware updates are necessary. Yet, the conventional firmware upgrade systems with centralized structure have a set of security threats, including integrity attacks, unauthorized access and scalability. Blockchain technology is a decentralized, tamper-proof and transparent method of securing firmware updates. The paper will provide a survey of the known blockchain-based systems of the secure update of firmware on the Internet of Things. We examined 36 scholarly articles, their proposed architectures, consensus mechanisms, security features, performance measures and limitations they may possess. Moreover, we have also found research gaps and proposed future research to improve blockchain-based firmware update processes.

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

1 INTRODUCTION

There is a significant revolution of the Internet of Things (IoT) in the contemporary infrastructure in various sectors such as healthcare, industrial automation, smart cities, agriculture and transportation systems. Connected IoT devices had reached 18 billion and are projected to reach about 29 billion devices by 2030 [2], highlighting the rapid dependence on connected ecosystems in all industries. It is projected that IoT devices will increase by 17.08 billion in 2024 to approximately 29 billion by 2030, as they will constantly gather, process and send data to improve the efficiency of operations, safety and convenience of the users. Nevertheless, this quickening growth has opened up serious security gaps especially in the firmware control and upgrade systems.

Firmware updates are the key to the success of IoT devices security as they allow manufacturers to address vulnerabilities and provide new functionality as well as stay compatible with new technological standards. The standard methods of Over-The-Air (OTA) firmware updates are based mostly on the centralized client-server models. Although these traditional deployment methods provide simplicity in implementation, they are characterized by several severe shortcomings: points of failure they have centralized update servers which are soft targets in cyberattacks and system downturns; integrity concerns because they do not have robust verification mechanisms so devices are vulnerable to maliciously injecting firmware and man-in-the-middle-attacks; lack of transparency as users and administrators cannot effectively observe the provenance of firmware, its version history and traces of modification; and scalability limitations where the centralized architecture cannot effectively deploy firmware across billions of heterogeneous devices.

Security of poor firmware management is dire and documented in abundance. The Verizon Data Breach Investigations Report states that an IoT device is involved in one of three data breaches today. More importantly, one of the main IoT security vulnerabilities is caused by unpatched firmware [1]. The nature of the IoT devices, being resource-constrained, further exacerbates these vulnerabilities with many devices having inadequate computational power, memory, and energy resources to enforce complex security. The growing complexity of cyber-attacks on IoT ecosystems requires new solutions that do not rely on the standard thinking about the centrality of anything. Researchers and practitioners have therefore started to investigate the use of decentralized solutions that can offer better security, scalability, and transparency to firmsware management in large-scale IoT systems.

Blockchain technology has become a disruptive methodology to solve these underlying problems. Blockchain can be used as an effective system of secure firmware management by relying on the principles of decentralization and cryptographic security, as well as the ability to create an immutable ledger. The technology has a number of very important benefits: it is decentralized, trust: this is achieved by removing central authorities with distributed consensus mechanisms; it is immutable, which is provided by the recording of all firmware versions and update histories in tamper-proof storage; it is transparent, which is achieved by verifiable audit trails of all the firmware transactions; it is secure, which is achieved by cryptographic hash functions to make sure that all the firmware is authentic; it is automated, such as smart contracts, to provide programmable logic to guarantee automated check of updates and distribution. These traits render blockchain especially well-adapted in order to mitigate the security issues inherent to the traditional firmware update systems. The blockchain market size in the global market in respect to the IoT was considered USD 761.03 million in 2024 and is expected to reach approximately USD 74,772.36 million by 2034 at a CAGR of 58.21 between 2025 and 2034 [2], which demonstrates that the market has well understood the potential of blockchain in IoT security.

Although there is increasing research focus, the field of blockchain-based firmware update systems is still splintered, with a large number of different approaches already making use of various blockchain systems like Ethereum, Hyperledger Fabric, and IOTA, and different consensus systems and system architectures. An in-depth overview of the solutions available should be conducted to find out the best practices, examine their effectiveness and inform future research directions.

The paper provides a syntactically and theoretically detailed survey of secure firmware update schemes of IoT devices, based on blockchain. The literature review considers a significant amount of peer-reviewed research publications published in 2017-2025, which reflects the latest developments in the topic. This work analyzes the framework architectures, the effectiveness of blockchain platforms, security improvements, and challenges of implementation through systematic evaluation using four research questions. The article conducts an in-depth comparison of solutions suggested in several dimensions such as blockchain platforms, consensus mechanisms, security, performance, and scalability. This review provides a critical synthesis of the current research by extracting common themes, architectural patterns, and new trends in the security of blockchain-based firmware. Moreover, full recognition of unexplored issues and research perspectives is intended to support the discipline. The discussion of practical implementation of the approaches based on the evaluation of the feasibility of real-world deployment, resource requirements, and trade-offs gives a practical understanding of the implementation. This review is a foundational source of information to all researchers, practitioners and policymakers wishing to comprehend, apply or further the blockchain based firmware update mechanisms within the IoT settings.

The rest of the paper is structured in the following way: Section III will feature connected literature related to blockchain-based firmware updates, and will review state-of-the-art methods in the recent literature. our systematic review approach, such as research questions, selection criteria, and analysis framework are highlighted in Section IV. Section V will be the comparative analysis and discussion of major findings in different dimensions. Section VI establishes important gaps and challenges in research. Lastly, Section VII wraps up the paper by providing insights and future research direction.

2 RELATED WORK

Ensuring secure firmware updates in IoT environments has been the focus of extensive recent research, utilizing decentralized storage, blockchain technology, and device-level authentication enhancements. Lin and Bo [1] proposed a pull-based firmware update mechanism for industrial IoT (IIoT) devices, leveraging IOTA Streams and IPFS. Their model addressed real-time update execution for low-capability IIoT devices, ensuring data integrity without traditional centralized servers. They also highlighted the importance of lightweight encryption and content addressing to maintain system resilience against DDoS attacks.

Sabarishraj et al. [2] built on this foundation and introduced an effective framework of Firmware Over-the-Air (FOTA) update with Raspberry Pi 4 and STM32 microcontrollers. They used hybrid encryption (AES + ECC), gzip compression, IPFS storage, and IPv6 VPN tunnels to maximize security and efficiency in transmission. Their approach was notable in terms of dealing with the constraints of devices through minimal computational loads and developing a conceptual UAV-based system of firmware delivery to devices with no Internet connectivity.The article by Sabarishraj et al. [2] built upon the latter and proposed an efficient Firmware Over-the-Air (FOTA) updates system using Raspberry Pi 4 and STM32 microcontrollers. They used hybrid encryption (AES + ECC), compression by gzip, storage with IPFS, and IPv6 VPN tunnels to maximize security and transmission efficiency. Their approach was notable, especially in light of the ability to overcome the limitations of the devices used in their experiments with a minimum quantity of computational resources required, and the concept of a UAV-delivery based firmware delivery framework was presented with devices not having Internet connectivity. At the same time, Biro and colleagues discussed blockchain-based dispatch systems to update firmware, and a conceptual framework of the UAV-based delivery system was introduced. Their work focused on scalable firmware integrity checking by Content Identifiers (CIDs) and focused on reducing the involvement of IoT devices by small, lightweight gateway nodes, and providing secure and reliable updates without imposing significant loads on devices.

In addition to these ideas, Joshi et al. [4] proposed a new PUF (Physical Unclonable Function)-based blockchain firmware update scheme. Their architecture was the first to use Device authentication using PUF-generated Challenge-Response Pairs (CRP) prior to being updated. Besides decentralizing firmware distribution through IPFS, this model also enhanced device identity validation and reduced the probability of malicious firmware injection which is usually ignored in previous models.

The other contribution [5] was also to add Software Bill of Materials (SBOM) metadata to a blockchain-based update model. Their system introduced supply-chain visibility, and devices were able to check firmware components before installation. This implementation method was complemented by blockchain inalterability and SBOM disclosure to increase protection against implicit vulnerabilities in third-party code, which represents a significant yet significantly under-reported attack surface in firmware delivery. Tinnaluri et al. [6], offered an effective model of data sharing by relying on blockchain-based IoT systems, which is secured. The model presented a decentralized trust architecture based on a consensus algorithm adapted to the IoT devices. They established better authentication and access control with better security and scalability without using centralized authorities by using overlay network structure with cluster heads and dynamic calculation of trust mechanism. Akkaoui [7] dedicated attention to the healthcare industry, which is the risk of fake IoMT (Internet of Medical Things) devices. She has created an authentication system based on smart contracts which utilizes Physical Unclonable Functions (PUFs) and the blockchain to guarantee the integrity of each device and safe software updates. This solution was implemented on Ethereum, and it guaranteed confidentiality, integrity, and man in the middle attack and replay attack resiliency, and was scalable, considering the computational capabilities of the medical IoT devices. The Firmblock architecture of firmware update introduced by the Study by Sey et al. [8] wrote on Ethereum provided all the previously mentioned features. Their solution was to integrate blockchain with a peer-to-peer IPFS storage model and a revocation system to deal with malware risks, attacks and the author disappearance issue. Firmblock improved firmware management in large IoT networks, in terms of robustness and scalability, by distributing update verification and securely revoking compromised device keys. The authors [9] suggested a security module supported with blockchain to convert regular inverters into smart inverters that have increased firmware security. They were designed to have an onboard security module (OSM) that performed the analysis of malware at rest and used Hyperledger Fabric to perform a secure firmware verification and recover in the event of an attack. They proved by experimental data that the implementation of the blockchain technology in inverter firmware systems increases resilience against firmware modification and malware injection attacks significantly. Sanchez-Gomez et al. [10] also made another significant advancement, having offered complete IoT architecture of safe lightweight communication, a firmware update and trust monitoring. To achieve a lightweight, interoperable, and secure communication in small-scale IoT conditions, their solution included LoRaWAN, OSCORE, SCHC compression, IPFS decentralized storage, and Hyperledger blockchain. The architecture especially focused on efficient over-the-air firmware updates and low-bandwidth and energy-constrained real-time trust monitoring. Fukuda and Omote [11] came up with an effective blockchain-based update scheme of firmware which can motivate distributors but with low computational and financial loads on the IoT devices. They use a smart contract and access control system as opposed to classic encryption and thus minimize gas costs and the complexity of key management. Protested implementation showed a significant savings of gas compared to the prior blockchain-based firmware distribution systems, providing an effective and scalable means of large-scale IoT deployment done at low cost. Mtetwa et al. [12], presented a blockchain-based system of updating firmware to LoRaWAN networks, aimed at resource-constrained devices. The approach that they propose is a combination of Ethereum blockchain and IPFS to guarantee authenticity, integrity, and availability of firmware without overloading low-power devices. Their effort to optimize cryptographic operations in a constrained environment provides evidence that blockchain can be viable to lightweight LPWAN IoT systems and enhances the quality of update delivery without resorting to the use of internet-intensive protocols. Hernandez-Ramos et al. [13] have conducted an extensive survey of the problem of updating firmware in IoT systems, including aspects such as version management, integrity protection, dependency tracking and trust management between a manufacturer and multiple software vendors. They critically examined attempts at standardization such as the IETF SUIT working group and suggested that blockchain might provide decentralized procedures to track updates and give security certifications to offset conventional secure firmware updates criteria.

Choi and Lee [14] suggested an architecture of a distributed firmware update based on blockchains which is an extension of IETF SUIT framework. Their model discusses the author-disappearing problem in a situation when manufacturers may not update because of the financial meltdown or because of a cyberattack. They remove single points of failure by storing firmware in blockchain and distributed file systems such as IPFS, guarantee availability of firmware, and can have resilient update mechanisms even in the absence of a manufacturer. Finally, Gao et al. [15] examined vulnerabilities to firmware security in microcontroller (MCU)-based IoT systems by researching based on real-world case studies. They exhibited physical attack vectors as well as remote attack vectors on vulnerable firmware update systems and pointed at their vulnerability in the case of the typical MCU environment. Moreover, they suggested and tested a secure prototype of a firmware update with AES encryption and authentication, which revealed possible pitfalls, such as clock glitch attacks, insecure key management, and failure to verify a firmware update completely, which provides crucial advice on how to secure the firmware update processes.

Ansay et al. [16] introduced Gnomon, a decentralized system with Decentralized Identifiers (DID) and verifiable credentials to register and update 5G IoT devices safely. Gnomon, which is based on Microsoft ION network and Sidetree, removes the traditional constraints of PKI by enabling devices to recover their identities and authenticate software distributions without the need to have centralized certificate authorities. Their implementation prototype showed both scalability and resiliency that is essential to massive 5G IoT implementations. Mtetwa et al. [17] created a secure framework of IoT firmware updates with the Ethereum blockchain smart contracts and IPFS (InterPlanetary File System) to store the firmware decentral. Their architecture attests to the integrity and authenticity of firmware with the help of a hash stored in smart contracts, thus allowing the IoT devices to retrieve updates on distributed IPFS nodes securely. Their use indicates that blockchain and smart contracts can protect update functions against man-in-the-middle attacks, rogue modifications, and central server outages. Yohan et al. [18] have proposed a lightweight framework of updating a firmware that uses skipchain technology that combines blockchain and skiplist frameworks. Their system also decentralizes the release and distribution of firmware by allowing peer-to-peer verification of firmware in a secure way between IoT devices and gateways. The two suggested protocols include secure firmware release and secure firmware distribution which shows efficient in scaling but with good firmware integrity protection with provision of lightweight cryptographic mechanisms which can be applied to the constrained IoT settings. Their design allows post-production feature customization (including upgrading IC features) by means of authenticated firmware through physical unclonable functions (PUFs) and blockchain registry. This solution represents a sustainable economic concept as it enables the dynamical upgrading and secures firware authenticity and safe ownership transfer throughout the lifecycle of a device. Witanto et al.

[20] built on the Open Connectivity Foundation (OCF) firmware update protocol, adding blockchain and smart contracts to enhance firmware integrity, transparency and efficiency of distribution. Their architecture guarantees the integrity of firmware by providing hash validation, based on blockchain technology, and provides a peer-to-peer method of updating, to improve availability and eliminate single points of failure, which is appropriate when using a large population of heterogeneous IoT devices.

He et al. [21] suggested a new architecture of grammar and compiler to implement automatically the creation of smart contracts to update the firmware based on Hyperledger Fabric. Their structure enables stakeholders to create, compile and interpret firmware update policies flexibly by writing formal specification grammar. Their system can greatly ease the errors of development on smart contracts to manage the IoT firmware and their testing indicates they complete their task successfully on various use cases. The PUSH based mechanism combining Hash Chain Verification and PUSH based model of Pillai et al. [22] is a blockchain based secure firmware update model. Their design relies on smart contracts as a means of checking the integrity of the firmware when distributed such that any manipulation through firmware manipulation can be easily identified even between versions. Their model enhances firmware delivery by strengthening against unauthorized modification and provides a transparent update lifecycle by keeping firmware update metadata in the blockchain.

The Son and Kim [23] suggested a Hyperledger Fabric architecture, which is a firmware management framework integrated with IPFS (InterPlanetary File System). They have a system that stores their firmware binaries and blockchain transactions independently to optimize storage and performance with references to the firmware that is immutable using blockchain records. In addition, they propose a broker system between the firmware vendors and the IoT consumers to have a flexible mechanism of updating and checking the firmware versions.

Kumar et al. [24] developed a complete security system of secure in-field OTA firmware updates on the IoT devices. Their model is a combination of JTAG security, hardware root-of-trust (with one-time programmable memory) and AES/RSA cryptographic protection. It ensures that not only firmware authenticity, but also intellectual property and embedded in the firmware is safeguarded through tight hardware security infrastructure and firmware update mechanism to reduce vulnerabilities such as reverse engineering, unauthorized firmware uploads, and side-channel attacks. Yohan and Lo [25] proposed an over-the-blockchain firmware update framework that can support not only direct, but also indirect firmware updates. Their system utilizes the concept of smart contracts to verify the authenticity and integrity of firmware and permit distribution of firmware by the manufacturer and third parties who serve as brokers. Their framework is scalable and resilient, unlike the previous models of centralized or Bitcoin-based models, by adopting Ethereum blockchain to achieve faster transaction confirmation and by supporting heterogeneous IoT environments through the support of OTA updates. Gupta [26] suggested a framework proposed to secure OTA updates in commercial IoT devices by adopting Ethereum blockchain. The vulnerability of the broken centralized servers was resolved with firmware hashes and references being saved in the blockchain, and the actual firmware files were distributed in IPFS. Tsaur et al. [27] proposed a very safe and effective blockchain-based system to update the firmware, minimizing the risk of MITM attacks and spoofed firmware injections. They addressed such problems as bandwidth constraints and authenticity of firmware with the help of Ethereum smart contracts and distributed storage networks. They created a model with functions such as the genesis nodes, manufacturer nodes and blockchain nodes to ensure control of the dissemination of firmware. The validation and antivirus measures were used to ensure that the clean firmware updates were provided to the IoT devices, and the RISK of malicious firmware was considerably reduced by the proposed over-the-blockchain framework of how the firmware updates should be delivered to devices. Yohan and Lo [28] offered the over-the-blockchain framework of the firmware updates delivery to the IoT devices, introducing the direct and indirect systems of firmware updates delivery. Their architecture consisted of vendor nodes, broker nodes and gateways whereby they used smart contracts to authenticate firmware integrity prior to its distribution. Their hybrid algorithm, which was a combination of two strategies (push- and pull-based updates), made their methods to be scalable, efficient, and with enhanced security in heterogeneous IoT networks, unlike the earlier centralized models. Lee and Lee [29] emphasized the use of blockchain technology in securing the firmware update of embedded IoT devices by proposing a peer-to-peer firmware sharing network. Their protocol enabled devices to examine both firmware versions and integrity in a decentralized blockchain consensus system.

It also included a feature to reduce attack windows through the process of ensuring embedded devices quickly received and approved firmware without overdependence on central servers, thereby boosting scalability for large-scale IoT deployments. Seo et al. [30] developed a blockchain-based firm-updating secure mechanism via UAVs. Identifying issues in regions with no internet connectivity, they employed private blockchain networks and UAVs as firmware-delivery intermediaries. Their architecture, developed on Hyperledger Fabric, consisted of operations such as participant enrollment, firmware verification, and secure communication based on public-key cryptography and Bloom filters. Their method particularly provided secure firmware updates even in rural and remote settings. Mtetwa et al. [31] have suggested a blockchain security model for LoRaWAN firmware updates. Their security model incorporates Blockchain and InterPlanetary File System (IPFS) to enable secure firmware transmission on constrained LoRaWAN networks. The solution addresses resource-constrained devices by providing integrity, confidentiality, authentication, and availability. The authors introduced a Firmware Update Service (FUS) to handle update orchestration and security during OTA firmware distribution. Experimental tests showed that their system is viable for constrained LoRaWAN implementations, providing secure protection against typical attacks.

He et al. [32] proposed a blockchain-supported OTA firmware update system for IoT devices to counter the intrinsic weakness of centralized update approaches. Their system utilizes smart contracts to validate firmware authenticity and avert Man-in-the-Middle (MitM) and Denial of Service (DoS) attacks. Deployed with Hyperledger Fabric and experimented on ESP8266 boards, the system under proposal confirmed the viability of blockchain-supported firmware updates without compromising performance significantly. The present contribution stresses that distributed verification with blockchain can effectively limit the single point of failure threats inherent in conventional OTA systems. Yohan and Lo [33] introduced FOTB (Firmware Over The Blockchain), a secure system providing PUSH and PULL update mechanisms for IoT devices. Their method combines consensus protocols and smart contracts to guarantee firmware integrity, authenticity, and timely delivery. FOTB facilitates third-party firmware vendors and provides peer-to-peer firmware update verification, effectively defending against firmware tampering, impersonation, and replay attacks. Formal security analysis proved that FOTB protects against significant cyber-attacks and realizes mutual authentication between devices and update servers. Anastasiou et al. [34] investigated a LoRa and Blockchain-based firmware update mechanism. Realizing the inadequacies of LoRa's low bandwidth and vulnerability to packet loss, they suggested adding blockchain-based verification to FUOTA (Firmware Update Over The Air) procedures. Their system employed smart contracts for verifying firmware authenticity and exploited LoRaWAN multicast capabilities to efficiently distribute firmware on mass IoT deployments. Performance analysis indicated that multiple cooperating gateways would be required for tolerable update times and reliability in large-scale deployments. Hernández-Ramos et al. [35] addressed the more general challenges and potential methods for securely updating IoT devices. They stressed key features such as integrity, confidentiality, versioning, dependency management, and recovery from failure. Their research also discussed two primary strategies: the IETF SUIT (Software Updates for Internet of Things) approach to standardizing secure firmware updates and blockchain-based designs for decentralized tamper-proof control of update processes. They promoted integrating lightweight cryptographic techniques with decentral technologies to effectively manage the life cycle of IoT firmware updates.

3 METHODOLOGY

This review article takes a systematic approach in identifying, analyzing, and summarizing the available literature on blockchain-based secure firmware update processes for IoT devices. A total of 36 papers were chosen through manual screening of peer-reviewed journals, conference publications, and preprint servers from 2017 to 2025. The inclusion was based on research that specifically dealt with firmware update processes using blockchain in IoT settings. Each paper was compared against four fundamental research questions that orchestrated this review, including the kinds of blockchain frameworks applied, their performance on updates, security features, and known challenges. A comparative analysis table was compiled to collate the methods, platforms, strengths, and weaknesses in all reviewed papers in an orderly manner. Also, a research questions map to the reviewed papers was made to verify the totality of the analysis. This approach guarantees that the review is exhaustive, clear, and consistent with existing trends in secure firmware update research via blockchain.

3.1 Objectives and Scope of the Study

The primary objective of this study is to conduct a comprehensive review of existing blockchain-based secure firmware update mechanisms tailored for Internet of Things (IoT) devices. The scope includes the examination of a broad range of solutions that leverage blockchain to ensure secure, verifiable, and scalable firmware delivery across heterogeneous IoT ecosystems. This review aims to:

- Identify and classify existing frameworks and approaches for secure firmware updates.
- Compare and analyze different blockchain platforms (e.g., Ethereum, Hyperledger, IOTA) used for firmware update purposes.
- Explore the security enhancements and limitations associated with these solutions.
- Highlight research gaps and propose future directions for improving blockchain-based firmware update mechanisms in IoT.

This review does not cover non-blockchain-based firmware update methods or solutions outside the IoT domain.

3.2 Research Questions

To guide the review process systematically, the following research questions (RQs) were formulated:

Table-1 Research Questions

ID	Research Questions
RQ1	What are the existing blockchain-based frameworks and models proposed for secure firmware updates in IoT environments?
RQ2	How do various blockchain technologies (e.g., Ethereum, Hyperledger, IOTA) impact the effectiveness and performance of secure firmware updates?
RQ3	What are the common security enhancements and limitations of existing blockchain-based firmware update mechanisms for IoT devices?
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 Inclusion Criteria

- Peer-reviewed research papers published in journals, conferences, and workshops.
- Papers proposing, evaluating, or discussing blockchain-based solutions specifically for firmware updates in IoT devices**.**
- Papers that provide technical and/or architectural insights into blockchain frameworks used for IoT firmware update security.
- Papers published between 2017 and 2025 to ensure relevance and currency of the reviewed solutions.

3.4 Exclusion Criteria

- Papers focusing on blockchain solutions not related to firmware updates.
- Non-peer-reviewed articles, blogs, white papers, and marketing materials.
- Papers that do not explicitly target IoT devices**.**
- Non-English language papers.
- Papers published before 2017, to maintain a focus on recent developments.

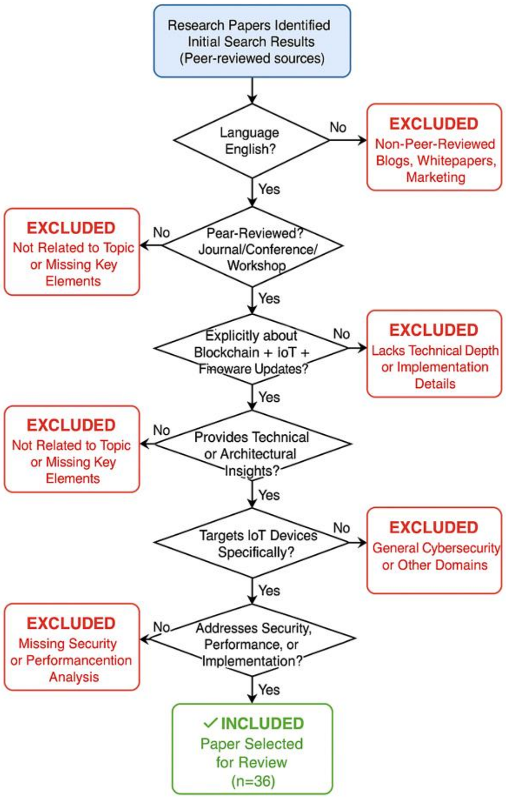

Figure 1: Systematic screening process for selecting peer-reviewed studies on blockchain-based IoT firmware update security. Each decision node filters papers by relevance, quality, and technical depth, leading to the final included set.

4 COMPARATIVE ANALYSIS AND DISCUSSION

Blockchain technology has been applied to IoT firmware security through various innovative approaches. Upon analyzing 36 research papers, several dominant themes and architectural trends emerge, each offering distinct advantages and facing unique challenges.

4.1 Decentralized Firmware Distribution and Verification

Many studies adopted decentralized models for distributing firmware updates using technologies like IPFS and blockchain smart contracts. These approaches eliminate centralized points of failure and ensure verifiable firmware integrity, but face scalability challenges for massive IoT networks.

4.2 Blockchain with Lightweight IoT Protocols

Frameworks targeting constrained devices integrated blockchain with low-power protocols like LoRaWAN. These designs optimized for resource efficiency but encountered trade-offs with update reliability and transmission delays.

4.3 Smart Contract-Based Secure Update Mechanisms

Smart contracts automate firmware verification and update authorization. Solutions like Ethereum and Hyperledger smart contracts provide decentralized control but introduce concerns regarding smart contract vulnerabilities and transaction costs.

4.4 PUF-Based Authentication and Hardware-Assisted Security

Incorporating Physical Unclonable Functions (PUFs) strengthens device identity verification before firmware updates. However, additional hardware requirements can increase deployment complexity and costs.

4.5 UAV and Hybrid Firmware Delivery Mechanisms

Emerging work proposes using UAVs and hybrid PUSH-PULL architectures to support firmware updates even in disconnected environments. While promising, these approaches introduce cost, operational, and security considerations for UAV-assisted systems.

5 RESEARCH GAPS

Despite significant progress, several research gaps remain in securing IoT firmware updates through blockchain. These gaps are evident even in recent peer-reviewed studies [1], [3], [4], [12], [19], [25], [30], [31], highlighting the evolving nature of this domain.

Despite significant progress, several research gaps remain in securing IoT firmware updates through blockchain:

5.1 Scalability and Performance

Studies such as [1], [3], and [31] show that current blockchain solutions do not scale efficiently for billions of IoT devices. Lightweight consensus mechanisms and Layer-2 blockchain solutions need further exploration. Current blockchain solutions do not scale efficiently for billions of IoT devices. Lightweight consensus mechanisms and Layer-2 blockchain solutions need exploration.

5.2 Energy Efficiency

As seen in [12] and [30], blockchain operations require considerable computational and energy resources, which is problematic for constrained IoT devices. Energy-optimized cryptographic techniques are lacking. Blockchain operations require considerable computational and energy resources, which is problematic for constrained IoT devices. Energy-optimized cryptographic techniques are lacking.

5.3 Cross-Platform Interoperability

Few studies like [4], [25] propose standardized, cross-platform solutions. Existing blockchain frameworks often remain vendor-specific or application-specific. Few studies propose standardized, cross-platform solutions. Existing blockchain frameworks remain vendor-specific or application-specific.

5.4 Secure Smart Contract Development

As noted in [3], [19], and [33], many proposals overlook the risks of poorly coded smart contracts, which themselves can become attack surfaces. Many proposals overlook the risks of poorly coded smart contracts, which themselves can become attack surfaces.

5.5 Secure Firmware Updates for Offline/Intermittently Connected Devices

Reliable methods for secure updates in low-connectivity environments require more research, especially leveraging blockchain's decentralized strengths.

5.6 Dynamic Trust Management

Current models assume static trust relationships. Dynamic, reputation-based trust models for firmware validation and update distribution need further investigation.

Recommendations and Suggestion:

This review comparatively examined 36 peer-reviewed scholarly articles published from 2017 to 2025 that are centered on blockchain-based secure firmware update systems for Internet of Things (IoT) devices. The research critically studied different blockchain frameworks like Ethereum, Hyperledger Fabric, and IOTA utilized to improve the firmware integrity, authenticity, and transparency. The analysis focused on major design trends including decentralized firmware delivery through IPFS, verification by smart contracts, and PUF-based trust management for device authentication. The review conducted a comprehensive comparison of architectural design, consensus algorithms, and performance metrics and shed light on the pros, cons, and trade-offs of each design. In total, it provides a systematic insight into the development of blockchain technology in resolving the shortcomings of centrally managed firmware update systems and gives an evidence-based integration of the state of the field of research in this area.

Even with great advancements, this review finds several gaps to be filled for secure, scalable, and energy-efficient firmware update systems using blockchain. Future research needs to work on lightweight consensus protocols and Layer-2 solutions for improving scalability for huge IoT networks. Energy-efficient cryptography, cross-platform compatibility, and smart contract design security using formal tools of verification need to be emphasized. Additionally, researchers need to investigate offline and delay-tolerant update protocols like UAV- or mesh-based firmware delivery for remote and sporadically connected IoT networks. Lastly, integrating AI-based anomaly detection and dynamic trust models could further enhance firmware integrity and operational resilience. Exploring these directions will lead the area toward practical, standardized, and globally deployable blockchain-based firmware update platforms for IoT ecosystems.

6 CONCLUSION

The proliferating use of IoT devices has highlighted the pressing need for secure, trustworthy, and scalable firmware update mechanisms. Conventional centralized methods have severe drawbacks including single points of failure, poor authenticity guarantees, and restricted traceability. This review systematically examined 36 research articles published between 2017 and 2025 that suggest blockchain-based solutions to improve the security of firmware updates for IoT systems.

By a systematic approach and comparative study, the research discovered some of the major trends. Decentralized verification, immutable logging, and support for smart contracts have made Ethereum, Hyperledger Fabric, and IOTA blockchain platforms widely used. Physical Unclonable Functions (PUFs), IPFS, and LoRa-based communication make these frameworks even more robust.

While considerable progress has been achieved, there are still important gaps in research, specifically about system scalability, energy efficiency, standardization, and management of intermittent connectivity. A single solution capable of resolving all these problems is elusive. Thus, future research must pursue hybrid models merging blockchain with light-consensus mechanisms, hardware-enabled trust anchors, and adaptive delivery schemes. Interdisciplinary solutions like this are necessary for providing end-to-end firmware integrity in large-scale, heterogeneous IoT environments.

This review is intended to provide a basis for future research and development within the field of secure IoT firmware updates, directing researchers and practitioners toward more resilient, decentralized, and reliable update mechanisms.

6.1.1.1.1 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 Biró, 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 Conversion 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 (SmartIoT)*, 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. Hernández-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 Omni-layer 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] S. Kumar, S. Sahoo, K. Kiran, A. K. Swain, and K. K. Mahapatra, "A Novel Holistic Security Framework for In-Field Firmware Updates," *2018 IEEE International Symposium on Smart Electronic Systems (iSES)*, IEEE, 2018.

[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 (BigDataSecurity)*, 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. Hernández-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].