International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)
https://ijcjournal.org/index.php/InternationalJournalOfComputer/index

A Methodology for Secure Remote Deployment of Internet of Things Devices Based on Cryptographic Authentication

Kydiuk Oleksandr*

Lead Software Engineer, Ukraine, Kiev
Email:o.p.kydiuk@globallogic.com

Abstract

The article is dedicated to the development of a methodological framework for secure remote deployment of Internet of Things devices based on cryptographic authentication. The relevance of the study is determined by the expansion of distributed IoT infrastructures, the growing dependence of industrial and service environments on remote device administration, and the rising exposure of connected endpoints to impersonation, firmware tampering, unauthorized enrollment, and trust-chain disruption. The scientific novelty lies in the integrated interpretation of remote deployment as a multi-phase cryptographic lifecycle rather than as an isolated provisioning event. The work describes the structural logic of identity provisioning, attestation-assisted trust establishment, secure channel creation, authenticated firmware distribution, and decentralized verification. Special attention is paid to hardware-backed onboarding, software-based attestation for constrained and legacy devices, segmented update delivery, and distributed trust validation. The work sets itself the goal of systematizing architectural and security principles that shape contemporary approaches to protected remote IoT deployment. To solve this task, comparative analysis, source synthesis, structural interpretation, and analytical generalization were used. The conclusion describes the transition toward lifecycle-oriented security models. The article will be useful for researchers, system architects, and engineers working with secure IoT infrastructures.

Keywords: Internet of Things; secure deployment; cryptographic authentication; remote attestation; firmware update; device provisioning; decentralized trust; secure onboarding; IoT security; certificate-based identity.

Received: 2/30/2026
Accepted: 4/30/2026
Published: 5/8/2026

---

* *Corresponding author.*

1. Introduction

The rapid expansion of Internet of Things infrastructures has significantly increased the number of distributed devices operating outside controlled physical environments. Industrial sensors, communication gateways, payment terminals, and embedded controllers frequently function for long periods without direct technical access, which makes secure remote deployment a critical operational requirement. In large-scale infrastructures, traditional factory-based provisioning models are no longer sufficient because static configuration mechanisms cannot ensure reliable authentication, secure software maintenance, or protection against unauthorized device enrollment.

Modern IoT ecosystems, therefore, increasingly rely on cryptographic authentication, remote attestation, and secure firmware management mechanisms to establish trust between devices and distributed network infrastructures. Remote deployment is gradually transforming from a simple provisioning procedure into a complex lifecycle process that integrates device identity formation, secure communication, integrity verification, and controlled firmware updates.

The purpose of this article is to analyze methodological approaches to secure remote deployment of Internet of Things devices based on cryptographic authentication. To achieve this purpose, the following objectives were formulated:

to identify the main architectural components of secure remote IoT deployment;

to analyze existing approaches to device identity provisioning, remote attestation, and secure firmware distribution;

to determine the main challenges and development directions of cryptographically protected deployment infrastructures.

The scientific novelty lies in the systematization of architectural principles of secure IoT deployment and in the interpretation of remote deployment as a unified cryptographic lifecycle integrating device identity provisioning, attestation, secure communication, and firmware lifecycle management. The research question addressed in the article is how secure remote deployment of IoT devices can be described as a sequence of cryptographic trust-establishment procedures rather than as a single provisioning operation. The article argues that deployment security depends on continuity between initial identity creation, attestation-based verification, authenticated communication, firmware update validation, and post-deployment integrity control.

2. Methods and materials

The materials for this study include scientific publications devoted to secure provisioning, remote attestation, firmware integrity verification, decentralized update distribution, and security architectures for Internet of Things systems.

The study of Sousa and his colleagues [1] examined secure provisioning and authentication mechanisms for IoT devices and evaluated the performance characteristics of cryptographic onboarding and secure communication infrastructures. The study of Ankergård and his colleagues [2] analyzed software-based remote attestation techniques for Internet of Things environments and identified their applicability to resource-constrained and legacy devices. The study of Gómez-Marín and his colleagues [3] proposed a remote enrollment architecture based on sealed cryptographic keys that allows attestation and credential generation to be performed simultaneously during device onboarding. The work of Catuogno and Galdi [4] investigated security challenges associated with firmware update mechanisms and described cryptographic approaches for protecting update authenticity and preventing rollback attacks. The study of Dirin and his colleagues [5] examined a multi-layer security framework designed to improve device integrity and data reliability within distributed IoT infrastructures. The work of Oktian and his colleagues [6] proposed a decentralized firmware update delivery system that distributes verification responsibilities across participating network nodes. The study of Yohan and his colleagues Reference [7] introduced a blockchain-based firmware update framework providing tamper-resistant verification of update authenticity. The research of Heeger and his colleagues. [8] analyzed secure firmware update mechanisms for LoRa networks using adaptive data rate techniques to improve update reliability in constrained wireless environments. The study of Mahfoudhi and his colleagues [9] examined over-the-air firmware update mechanisms for NB-IoT devices operating under strict communication and memory constraints. The work of Gu and his colleagues. [10] proposed a firmware update framework designed for large multi-hop industrial IoT networks based on IEEE 802.15.4 DSME communication architecture. The selection of studies was based on their direct relevance to at least one phase of the remote deployment lifecycle: provisioning, authentication, remote attestation, firmware update protection, constrained-network update delivery, decentralized verification, or multi-layer IoT integrity governance. Priority was given to peer-reviewed journal publications published between 2021 and 2025, because this period reflects the transition from isolated onboarding mechanisms toward lifecycle-oriented deployment architectures.To prepare the article, source analysis, comparative analysis, synthesis of research results, and analytical generalization were used. These methods made it possible to identify common methodological patterns and architectural principles underlying secure remote deployment of IoT devices.

3. Results

The analytical reconstruction of contemporary approaches to secure remote deployment of Internet of Things devices reveals a gradual transformation of device lifecycle management models. Instead of treating device provisioning as a static manufacturing-stage operation, recent architectures reinterpret deployment as a continuous cryptographically governed process that integrates authentication, remote integrity verification, firmware lifecycle control, and scalable infrastructure orchestration. Within this evolving landscape, several structural regularities emerge: the centrality of device identity formation, the reliance on cryptographic bootstrapping during the onboarding phase, and the progressive decentralization of trust verification mechanisms. The systematization of methodological directions is presented below (Table 1).

Table 1: Structural components of secure remote IoT deployment methodology (compiled by the author based on [1-7])

Methodological direction	**Functional purpose in deployment architecture**	**Security contribution**	**Operational implication**
Cryptographic identity provisioning	Establishes a unique device identity during onboarding	Prevents impersonation and unauthorized enrollment	Forms the initial trust anchor for further interaction
Remote attestation	Verifies device software state after deployment	Detects integrity violations and compromised runtime states	Extends trust assessment beyond initial registration
Secure channel formation	Protects device-to-platform and device-to-device exchanges	Preserves confidentiality, integrity, and authenticity of traffic	Enables protected command delivery and service access
Firmware authenticity control	Validates the update origin and software legitimacy	Blocks malicious modification and rollback scenarios	Maintains security continuity during lifecycle changes
Segmented update orchestration	Adapts software delivery to constrained communication environments	Reduces exposure during fragmented transmission	Supports reliable updates in NB-IoT, LPWAN, and similar networks
Distributed trust verification	Redistributes validation functions across nodes or authorities	Reduces dependence on a single verification point	Improves the resilience of large-scale infrastructures
Multi-layer integrity governance	Links device authentication with data and system integrity controls	Strengthens defense against coordinated attacks	Connects device security with platform-level reliability

The classification given above clarifies that secure deployment is organized not around a single protective measure but around a sequence of interdependent verification and control functions. One of the most persistent structural problems identified across implementations concerns the formation of device identity at scale. In distributed IoT environments where thousands or millions of nodes operate simultaneously, the absence of reliable identity provisioning creates systemic vulnerabilities, enabling impersonation attacks and unauthorized network participation. Identity provisioning schemes, therefore increasingly rely on hardware-backed cryptographic tokens and certificate infrastructures capable of establishing trust anchors at the moment of device onboarding. A cryptographic provisioning architecture integrating secure tokens with public-key infrastructure has demonstrated

that identity creation, authentication, and secure communication channels can be established during the provisioning stage with an average runtime of 1137.8 ms ±65.11, with manager-side cryptographic operations requiring 615.1 ms ±9.01 and client-side operations 522.7 ms ±56.1 under controlled conditions [1]. The significance of these measurements lies not merely in performance metrics but in demonstrating that cryptographically strong onboarding procedures remain computationally feasible even on low-power IoT platforms.

A second structural regularity emerges around the problem of remote device integrity verification. The distributed nature of IoT deployments dramatically expands the attack surface, especially in infrastructures composed of heterogeneous and resource-constrained devices. Remote attestation techniques, therefore, play a central role in establishing device trustworthiness after deployment. Software-based remote attestation schemes demonstrate that device state verification can be achieved through runtime integrity proofs without requiring specialized hardware modules, an approach particularly relevant for legacy or low-cost IoT nodes that lack trusted execution environments [2]. The architectural implication is significant: secure deployment methodologies must account for the coexistence of hardware-secured and software-verified trust anchors within the same network. Such hybrid verification layers enable security enforcement even when hardware root-of-trust mechanisms cannot be deployed retroactively.

The third major pattern concerns the secure distribution of firmware updates. Once devices are operational, maintaining their security state requires controlled mechanisms for remote firmware modification. Firmware update protocols designed for low-power wide-area networks demonstrate that cryptographically protected update pipelines must balance security guarantees with strict bandwidth constraints. Secure LoRa firmware update mechanisms, for instance, adapt transmission parameters dynamically in order to reduce update latency and maintain communication reliability across constrained wireless links [8]. These approaches illustrate how update delivery protocols must integrate both cryptographic verification and adaptive network control mechanisms to remain effective in heterogeneous IoT environments.

A complementary trajectory can be observed in the development of remote enrollment mechanisms that integrate attestation with cryptographic key sealing. Systems based on sealed-key enrollment architectures enable a device to establish a trusted identity without exposing its private cryptographic material during registration. In such frameworks, attestation and key provisioning are performed simultaneously, allowing the remote platform to validate device integrity while issuing credentials that remain cryptographically bound to the device state [3]. This convergence of enrollment and attestation procedures reduces the risk of compromised devices entering the trusted network domain and illustrates a broader shift toward multi-stage authentication pipelines in IoT deployment methodologies.

The complexity of firmware lifecycle management becomes particularly visible when examining constrained cellular IoT environments such as NB-IoT networks. Over-the-air update protocols designed for these environments demonstrate that update fragmentation, retransmission management, and integrity validation must be coordinated across devices with extremely limited memory and transmission bandwidth. Secure firmware distribution strategies, therefore, rely on segmented update packages combined with cryptographic verification

mechanisms to ensure reliability while minimizing communication overhead [9]. Such architectures illustrate that secure remote deployment is inseparable from update distribution mechanisms capable of sustaining device integrity throughout operational lifecycles.

Security analysis of firmware update pipelines reveals additional architectural constraints. Firmware modification mechanisms must simultaneously guarantee the authenticity of update packages, the integrity of transmitted data, and resistance to rollback attacks. Cryptographic frameworks developed for secure firmware distribution demonstrate that authentication chains, digital signatures, and version-tracking mechanisms are required to prevent unauthorized software modification or downgrade attacks [4]. Without these safeguards, remote deployment infrastructures risk becoming vectors for large-scale compromise rather than instruments of maintenance and resilience.

The broader architectural layer of IoT infrastructures introduces additional requirements concerning data integrity and device state validation. Security frameworks designed for distributed IoT systems highlight the necessity of multi-layer integrity controls combining network authentication, device verification, and data integrity monitoring. In such frameworks, the interaction between device authentication protocols and system-level integrity mechanisms becomes the primary factor determining the resilience of IoT infrastructures against coordinated attacks [5]. Device-level cryptographic authentication, therefore, functions as only one element within a larger verification ecosystem that must continuously validate system behavior.

Scalability considerations become particularly prominent when firmware distribution mechanisms must operate across large industrial IoT networks. Multi-hop communication environments, especially those built on IEEE 802.15.4 DSME networks, require firmware distribution protocols capable of propagating updates through large device topologies without overloading network resources. Firmware-over-the-air frameworks designed for such networks demonstrate that distributed scheduling and coordinated transmission windows significantly improve update reliability across multi-hop infrastructures [10]. These approaches confirm that secure deployment architectures must incorporate network-aware distribution strategies when operating at an industrial scale.

Decentralized firmware distribution introduces an additional architectural dimension by eliminating single points of failure in update infrastructures. Blockchain-based update delivery frameworks demonstrate that distributed verification mechanisms can ensure the authenticity of firmware packages while maintaining a tamper-resistant audit trail of update events. Such architectures rely on distributed ledgers to store firmware hashes and update records, enabling devices to verify update authenticity independently of centralized authorities [7]. The introduction of decentralized verification layers, therefore, addresses one of the most persistent structural weaknesses in traditional IoT deployment architectures: the vulnerability of centralized update servers.

An intermediate approach between centralized update infrastructures and blockchain-based verification systems is represented by decentralized firmware distribution services integrated directly into IoT networks. Secure decentralized update delivery frameworks distribute update verification responsibilities across participating nodes, enabling the system to validate firmware authenticity collectively rather than relying on a single authority Reference [6]. This architectural model reduces the operational risks associated with centralized infrastructure

compromise and reflects a broader trend toward distributed trust management in large-scale IoT ecosystems. When these trajectories are examined collectively, a coherent methodological structure becomes visible. The generalized deployment logic is presented below (Figure 1).

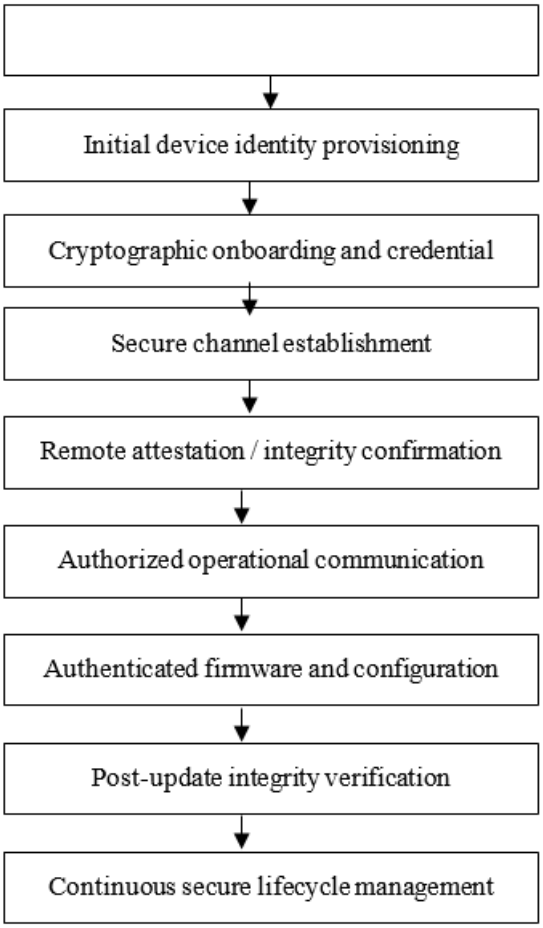

Figure 1: Scheme of the cryptographic lifecycle of secure remote IoT deployment (compiled by the author based on [1-5, 9])

This sequence makes visible that the deployment process develops as a closed cryptographic lifecycle in which each subsequent stage depends on the validity of the preceding trust decision. Secure remote deployment of IoT devices emerges as a multi-phase cryptographic lifecycle consisting of device identity provisioning, attestation-based trust establishment, authenticated communication channel formation, secure firmware distribution, and continuous device integrity monitoring. Each stage reinforces the others: identity provisioning establishes the initial trust anchor, attestation mechanisms confirm device integrity, encrypted communication protects operational data flows, and firmware update infrastructures maintain system security throughout the device lifecycle.Another pattern becomes evident when examining the energy and performance characteristics of cryptographic deployment procedures. Empirical measurements indicate that the additional computational cost associated with cryptographic onboarding procedures remains relatively small in comparison with baseline device energy consumption. For example, cryptographic operations performed during authentication processes increase energy usage by only 0.4 Wh, while baseline system consumption during idle operation remains at approximately

2.2 Wh [1]. Such results indicate that cryptographically secure onboarding procedures can be integrated into low-power IoT infrastructures without significantly affecting operational energy budgets.

Scalability results obtained from authentication validation infrastructures further reinforce the feasibility of large-scale deployment models. The numerical distribution of the measured indicators is presented below (Figure 2).

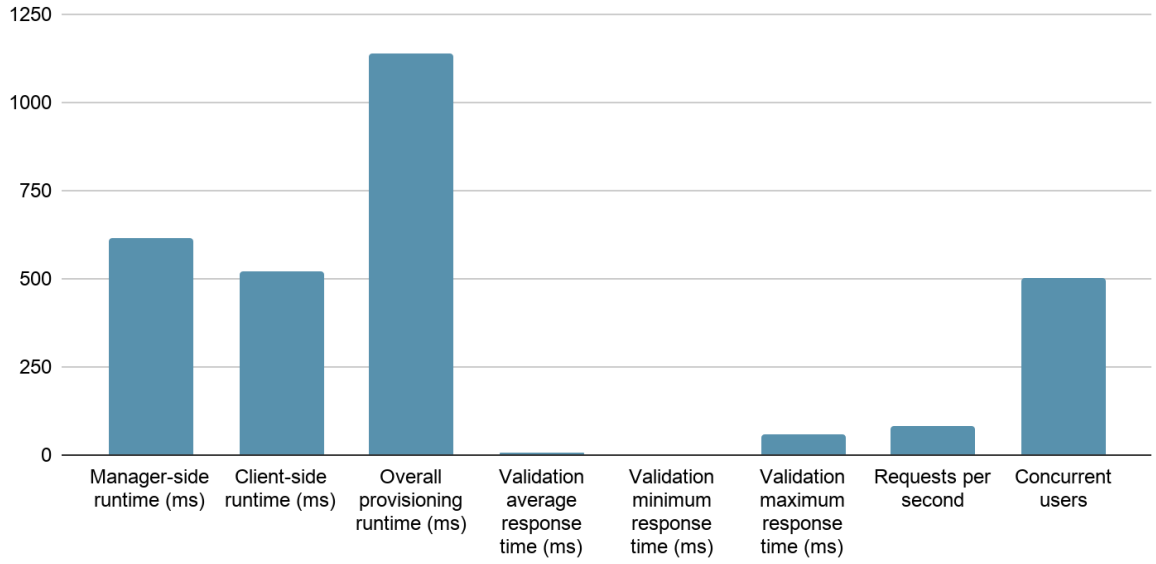

Figure 2: Numerical profile of authentication and validation performance in secure remote IoT deployment (compiled by the author based on [1])

Placed in one visual field, these values show that the most resource-intensive phase remains the provisioning sequence itself, whereas the validation layer operates with substantially lower response latency even under concurrent load. Under simulated load conditions involving 500 concurrent users with a spawn rate of 0.5 users per second, authentication validation services demonstrate an average response time of 4.55 ms, with a minimum of 0.84 ms and a maximum of 59.40 ms, while sustaining 83.86 requests per second [1]. These measurements confirm that secure authentication services can support large device populations without introducing prohibitive latency.

The integration of these mechanisms results in a deployment paradigm where IoT devices are no longer treated as static endpoints but as cryptographically governed participants in a continuously verified network ecosystem. Device authentication, remote attestation, firmware distribution, and trust verification operate as interdependent layers within a single deployment methodology. The resulting architecture combines hardware-assisted security, software-based integrity verification, scalable update mechanisms, and distributed trust infrastructures, forming the basis for secure remote deployment strategies capable of sustaining large-scale IoT infrastructures under evolving security conditions.

4. Discussion

The analytical results reveal a structural shift in the conceptualization of Internet of Things device deployment. Earlier IoT infrastructures were designed around static provisioning models where devices were configured during manufacturing and subsequently operated within relatively fixed trust boundaries. Contemporary distributed environments no longer support such assumptions. The rapid growth of heterogeneous IoT ecosystems, coupled with the geographic dispersion of devices and the sensitivity of the data they process, has made static provisioning architectures operationally and security-wise insufficient. The analytical synthesis presented in the Results section indicates that modern deployment frameworks increasingly treat device onboarding as a cryptographically controlled lifecycle event rather than a one-time configuration step.

Previous studies examine secure remote deployment through several separate research lines. Provisioning and authentication research explains how the initial trust anchor is created during onboarding [1], while remote attestation studies show how device integrity can be verified after deployment, including in systems without specialized hardware modules [2]. Sealed-key enrollment models connect these two directions by combining credential issuance with device-state verification [3]. Firmware update studies shift attention to the later phases of the lifecycle, where digital signatures, version control, rollback protection, and constrained-network delivery mechanisms preserve device integrity after software modification [4, 8–10]. Decentralized and blockchain-based update frameworks add another layer by reducing dependence on a single update authority and improving traceability of firmware validation events [6, 7]. The contribution of the present article lies in connecting these previously separated directions into one methodological lifecycle model.

The central implication of this transformation lies in the redefinition of device identity management. Previous architectures frequently relied on shared secrets or static identifiers embedded during manufacturing. Such mechanisms, although operationally simple, created systemic vulnerabilities because compromised credentials could be reused across multiple nodes or networks. Recent security frameworks instead emphasize device-specific cryptographic identities generated during the onboarding phase. The analytical evidence shows that certificate-based infrastructures, when combined with secure tokens or hardware-protected cryptographic modules, significantly reduce the probability of impersonation attacks and unauthorized enrollment. This shift toward cryptographically verifiable identities effectively transforms the device provisioning phase into the primary moment of trust establishment within IoT ecosystems.

Another important analytical observation concerns the relationship between identity provisioning and remote attestation mechanisms. Earlier security models tended to treat authentication and integrity verification as separate processes. However, modern IoT environments increasingly combine these mechanisms into unified verification pipelines. Remote attestation techniques allow the network to verify not only the identity of a device but also the integrity of its software environment. This dual verification model is particularly relevant for large-scale infrastructures where devices may operate unattended for long periods and may be physically accessible to adversaries. The integration of attestation into deployment methodologies, therefore reflects an emerging recognition that trust in distributed systems cannot be based solely on identity credentials; it must also incorporate evidence about device state and software integrity.

The evolution of firmware lifecycle management represents another important dimension of secure deployment architectures. Historically, firmware updates were treated as maintenance procedures executed manually or through proprietary update mechanisms. In contemporary IoT infrastructures, firmware updates are increasingly interpreted as security-critical operations requiring cryptographic validation, integrity checks, and controlled distribution channels. Analytical evidence suggests that secure firmware update mechanisms now integrate digital signatures, version validation systems, and rollback protection policies to prevent malicious software installation. This transformation indicates that secure deployment methodologies must encompass not only the initial onboarding of devices but also their entire operational lifecycle, including remote updates and configuration changes.

Scalability considerations also significantly influence the architecture of secure deployment systems. Early IoT security models were designed for relatively small networks where centralized authentication servers could manage device credentials and authorization decisions. As device populations expanded into the millions, centralized verification infrastructures began to reveal structural limitations. High-scale networks require authentication and verification processes capable of operating under heavy concurrency without creating bottlenecks or single points of failure. The analysis indicates that distributed verification architectures, hierarchical certificate chains, and decentralized trust anchors increasingly replace purely centralized identity management systems. These architectural shifts allow networks to authenticate and manage devices in parallel while preserving cryptographic integrity.

The introduction of decentralized verification models also addresses another long-standing problem in IoT infrastructures: the vulnerability of centralized update or authentication services. In systems where a single authority manages firmware updates or identity verification, the compromise of that authority can jeopardize the entire network. Distributed trust architectures mitigate this risk by distributing verification responsibilities across multiple nodes or authorities. Blockchain-based update verification systems and decentralized firmware distribution frameworks represent two examples of this architectural evolution. Although such solutions introduce additional complexity and computational overhead, they significantly improve the resilience of large-scale IoT ecosystems against coordinated attacks targeting centralized infrastructure.

A further observation emerging from the analytical synthesis concerns the role of hardware-assisted security mechanisms. Trusted hardware modules, secure tokens, and hardware security modules contribute to the protection of cryptographic keys and authentication procedures. Hardware-backed cryptographic operations provide strong guarantees against key extraction attacks because private keys remain isolated from general-purpose operating systems. However, the analysis also demonstrates that exclusive reliance on hardware trust anchors is not always feasible. Many legacy IoT devices lack the computational resources or architectural support required for advanced trusted execution environments. Consequently, modern deployment methodologies often combine hardware-assisted and software-based verification mechanisms, allowing security guarantees to be extended across heterogeneous device populations.

Energy efficiency and computational constraints represent additional design considerations for secure deployment frameworks. IoT devices frequently operate in resource-constrained environments where processing power,

memory capacity, and energy consumption are strictly limited. Cryptographic authentication procedures must therefore be optimized to avoid excessive overhead. Analytical findings indicate that elliptic-curve cryptographic algorithms are particularly well suited for such environments because they provide strong security guarantees while requiring significantly smaller key sizes and computational resources compared with classical public-key algorithms. These characteristics explain their widespread adoption in secure onboarding and communication protocols within IoT infrastructures.

Another dimension that emerges from the analysis concerns network heterogeneity. IoT ecosystems often incorporate devices communicating through different networking technologies, including low-power wide-area networks, cellular IoT infrastructures, and local wireless protocols. Secure deployment architectures must therefore be compatible with diverse communication conditions, bandwidth limitations, and latency characteristics. Adaptive firmware distribution mechanisms and segmented update delivery strategies have been developed to address these challenges. These techniques allow update packages to be transmitted efficiently even across constrained networks where traditional update methods would be impractical.

The broader implication of these observations is that secure remote deployment is no longer a single technical procedure but rather a composite architectural process involving multiple interacting subsystems. Identity provisioning, attestation mechanisms, communication encryption, firmware update infrastructures, and authorization policies collectively define the security posture of an IoT deployment. Each component influences the reliability of the others, and weaknesses in any single layer can compromise the entire system. Consequently, effective deployment methodologies must be designed as integrated security frameworks rather than collections of independent protective mechanisms.The synthesis of previous research, therefore indicates that secure remote deployment methodologies are evolving toward comprehensive lifecycle security models. These models integrate identity provisioning, cryptographic authentication, attestation protocols, and firmware lifecycle management into unified frameworks capable of supporting large-scale IoT infrastructures. At the same time, unresolved challenges related to scalability, interoperability, continuous monitoring, and infrastructure management suggest that secure deployment remains an active and rapidly developing research domain within the broader field of Internet of Things security.

The study has several limitations. First, it is based on analytical synthesis of published research and does not present a new experimental deployment of IoT devices. For this reason, the proposed lifecycle model should be interpreted as a methodological framework rather than as a directly benchmarked implementation. Second, the analyzed studies examine different device classes, communication protocols, and deployment environments, including provisioning infrastructures, remote attestation schemes, LoRa update procedures, NB-IoT firmware delivery, blockchain-based verification, and industrial multi-hop update frameworks. This heterogeneity limits direct quantitative comparison between the reported results. Third, the article focuses mainly on cryptographic authentication, attestation, secure channel formation, firmware update protection, and distributed verification; physical tamper resistance, supply-chain inspection, organizational incident response, and legal compliance remain outside the scope of the analysis. Future research should test integrated deployment architectures in large-scale experimental or simulated environments and measure latency, energy consumption, update reliability, certificate revocation efficiency, and resistance to coordinated compromise.

5. Conclusion

The conducted analysis demonstrates that secure remote deployment of Internet of Things devices is evolving toward lifecycle-oriented security architectures that combine device identity provisioning, cryptographic authentication, remote attestation, and secure firmware management.

The first objective was achieved through the identification of the main architectural components of secure deployment, including identity formation, secure communication channels, integrity verification, and authenticated firmware update mechanisms. The second objective was fulfilled by analyzing how contemporary studies explain the interaction between provisioning procedures, attestation mechanisms, and update infrastructures within distributed IoT environments. The third objective was accomplished through the identification of major limitations of current approaches, including scalability challenges, infrastructure management complexity, interoperability issues, and computational constraints of low-power devices.

The results confirm that secure remote deployment should be interpreted not as a single configuration step but as a continuous cryptographic lifecycle ensuring the integrity, authenticity, and reliability of Internet of Things infrastructures throughout the entire operational period of connected devices.

Acknowledgements

These and the Reference headings are in bold. Text below continues as normal.

References

[1]. Sousa, P. R., Magalhães, L., Resende, J. S., Martins, R., & Antunes, L. (2021). Provisioning, authentication, and secure communications for IoT devices on FIWARE. *Sensors, 21*(17), 5898. https://doi.org/10.3390/s21175898

[2]. Ankergård, S. F. J. J., Dushku, E., & Dragoni, N. (2021). State-of-the-art software-based remote attestation: Opportunities and open issues for Internet of Things. *Sensors, 21*(5), 1598. https://doi.org/10.3390/s21051598

[3]. Gómez-Marín, E., Parrilla, L., Mauro, G., Escobar-Molero, A., Morales, D. P., & Castillo, E. (2022). RESEKRA: Remote enrollment using sealed keys for remote attestation. *Sensors, 22*(13), 5060. https://doi.org/10.3390/s22135060

[4]. Catuogno, L., & Galdi, C. (2023). Secure firmware update: Challenges and solutions. *Cryptography, 7*(2), 30. https://doi.org/10.3390/cryptography7020030

[5]. Dirin, A., Oliver, I., & Laine, T. H. (2023). A security framework for increasing data and device integrity in Internet of Things systems. *Sensors, 23*(17), 7532. https://doi.org/10.3390/s23177532

[6]. Oktian, Y. E., Le, T.-T.-H., Jo, U., Laksmono, A. M. A., & Kim, H. (2024). Secure decentralized firmware update delivery service for Internet of Things. *Internet of Things, 26*, 101136. https://doi.org/10.1016/j.iot.2024.101136

[7]. Yohan, A., Lo, N. W., & Santoso, L. P. (2025). A robust and efficient blockchain-based framework for updating firmware in IoT environments. *Peer-to-Peer Networking and Applications, 18*, 207.

https://doi.org/10.1007/s12083-025-02031-7

[8]. Heeger, D., Garigan, M., Tsiropoulou, E., & Plusquellic, J. (2021). Secure LoRa firmware update with adaptive data rate techniques. *Sensors, 21*(7), 2384. https://doi.org/10.3390/s21072384

[9]. Mahfoudhi, F., Sultania, A. K., & Famaey, J. (2022). Over-the-air firmware updates for constrained NB-IoT devices. *Sensors, 22*(19), 7572. https://doi.org/10.3390/s22197572

[10]. Gu, J., Lee, S.-S., & Kang, H. (2024). DSME-FOTA: Firmware over-the-air update framework for IEEE 802.15.4 DSME MAC to enable large-scale multi-hop industrial IoT networks. *Internet of Things, 27*, 101239. https://doi.org/10.1016/j.iot.2024.101239