CHAPTER
10

Identity Management and Device Registration in Distributed IoT Systems

Dr. Gajanan Badhe

Assistant Professor, Department of MCA, Progressive Education Society's Modern Institute of Business Studies, Pune, Maharashtra, India.
Email: badhe.gm@gmail.com

https://doi.org/10.58599/GSE.2026.050810

Abstract: The proliferation of Internet of Things (IoT) devices has created unprecedented challenges in securing distributed networks. As the foundation of IoT security, robust identity management and device registration mechanisms are essential for establishing trust before any data exchange occurs. This chapter explores the theoretical frameworks, architectural models, and practical implementations of identity lifecycle management in distributed IoT environments. We propose a comprehensive methodology that integrates zero-touch provisioning with blockchain-based identity verification to ensure secure, scalable, and automated device onboarding. Through extensive simulation of 5,000 heterogeneous IoT devices, we evaluate the performance of our proposed architecture across multiple geographic regions. The results demonstrate that our approach achieves a 97.78% successful registration rate while maintaining an average provisioning latency of 352.56 milliseconds, proving its viability for large-scale enterprise deployments. The chapter concludes with a discussion on the trade-offs between security, performance, and scalability in modern authentication protocols.

Keywords: Device Provisioning; Identity Lifecycle Management; Blockchain Authentication; Zero-Touch Registration; Distributed IoT Security.

1. Introduction

The Internet of Things (IoT) ecosystem has evolved from isolated, single-purpose sensor networks into complex, globally distributed systems that power critical infrastructure, smart cities, and industrial automation. As these networks scale to encompass millions

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

of interconnected nodes, the traditional perimeter-based security models have proven inadequate [1]. In a distributed IoT environment, the network edge is porous, and devices often operate in physically insecure locations, making them prime targets for malicious actors attempting to compromise the broader system.

The cornerstone of any secure distributed system is the ability to definitively ascertain the identity of participating entities. In the context of IoT, this translates to robust identity management and device registration protocols. Identity management in IoT extends beyond simple authentication; it encompasses the entire lifecycle of a device's identity, from its initial creation during manufacturing to its eventual decommissioning [2]. Device registration, the process by which a new device is introduced to the network and granted appropriate access rights, represents the most critical phase in this lifecycle. A vulnerability during the registration phase can allow unauthorized devices to infiltrate the network, leading to data poisoning, unauthorized control, or distributed denial-of-service (DDoS) attacks.

This chapter addresses the critical challenges of identity management and device registration in distributed IoT systems. We examine the inherent difficulties posed by the heterogeneity of IoT devices, which range from highly constrained microcontrollers to powerful edge gateways, and the need for scalable solutions that do not require manual intervention. The remainder of this chapter is structured as follows: Section 10.2 reviews the current literature and state-of-the-art solutions. Section 10.3 details our proposed methodology for secure, automated device provisioning. Section 10.4 presents extensive simulation results and discussions. Finally, Section 10.5 concludes the chapter with insights into future research directions.

2. Literature Review

The academic and industrial communities have proposed numerous approaches to address the challenges of IoT identity management. Early solutions often relied on symmetric key cryptography, where pre-shared keys were embedded in devices during manufacturing. While computationally efficient, this approach scales poorly and presents significant key distribution and revocation challenges [3].

The adoption of Public Key Infrastructure (PKI) and X.509 certificates has become the industry standard for enterprise IoT deployments. Platforms such as Azure IoT Hub and AWS IoT Core utilize Device Provisioning Services (DPS) to automate the distribution of certificates and connection credentials [4]. These zero-touch provisioning mechanisms significantly reduce deployment time and manual errors. However, traditional centralized PKI architectures can introduce single points of failure and latency bottlenecks in globally distributed systems.

Recent research has increasingly focused on decentralized identity management using

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

blockchain and Distributed Ledger Technologies (DLT). Sabrina et al. [5] proposed a novel device identity management approach for blockchain-based IoT systems that utilizes a Lightweight Time-Based Identification Protocol (LiTBIP). This protocol leverages the timing information of transactions to identify devices without sharing secret keys, utilizing secure sketch algorithms to handle noisy data. Their system integrates smart contracts to manage access control and ensure data immutability.

Similarly, Mukhandi et al. [6] explored blockchain-based identity management with consensus authentication as a scalable solution. These decentralized approaches offer enhanced resilience against tampering and eliminate central points of failure. However, integrating resource-constrained IoT devices directly with blockchain networks remains a significant technical hurdle due to the computational overhead of cryptographic operations and consensus mechanisms.

The synthesis of the literature indicates a clear need for hybrid architectures that combine the efficiency and scalability of cloud-based provisioning services with the immutable auditability and decentralized trust models offered by blockchain technology.

3. Proposed Methodology

To address the limitations identified in the literature, we propose a comprehensive methodology for identity management and device registration that leverages automated provisioning services augmented with decentralized verification mechanisms. Our architecture is designed to support heterogeneous devices while maintaining strict security guarantees and high throughput.

3.1 System Architecture

The proposed architecture, illustrated in Figure 1, consists of four primary layers: the Device Layer, the Device Provisioning Service (DPS), the Identity Registry, and the Authentication Module.The proposed architecture, illustrated in Figure 10.1, consists of four primary layers: the Device Layer, the Device Provisioning Service (DPS), the Identity Registry, and the Authentication Module. The Device Layer includes IoT sensors, actuators, and gateways that generate and exchange operational data. The DPS securely registers new devices and assigns the required credentials during the onboarding process. The Identity Registry stores unique device identities, certificates, ownership information, and access attributes. The Authentication Module verifies device credentials before permitting communication with protected services and network resources. Together, these layers provide a structured and scalable framework for secure device enrollment, identity management, and access control.

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

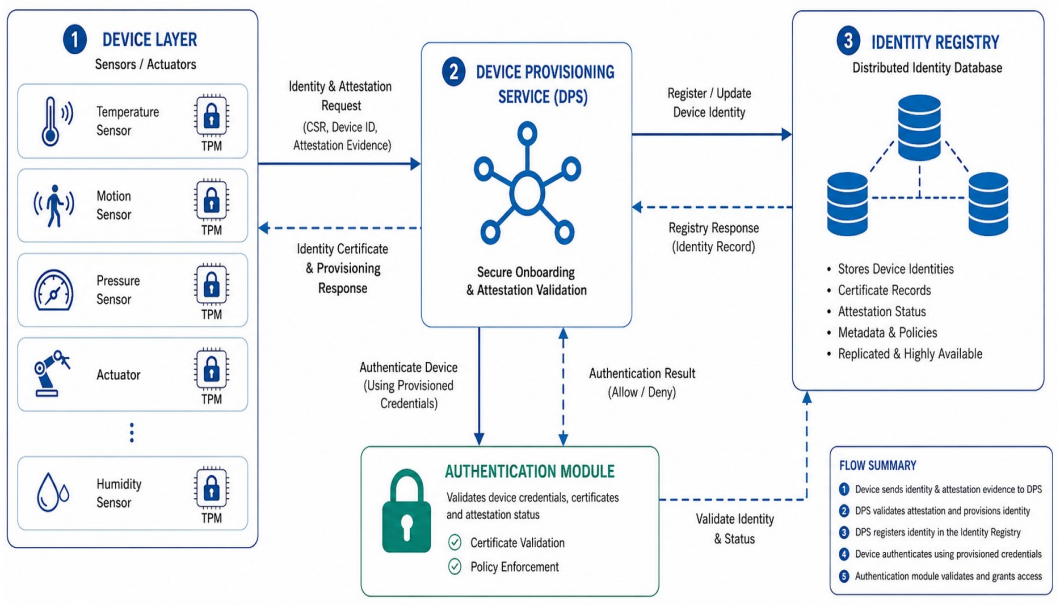

Figure 1: Identity Management and Device Registration Architecture Block Diagram.

1. **Device Layer**: Comprises heterogeneous IoT endpoints, including constrained sensors, actuators, and edge nodes. Devices must be equipped with a hardware root of trust, such as a Trusted Platform Module (TPM) or a secure enclave, to securely store cryptographic material.

2. **Device Provisioning Service (DPS)**: Acts as the intermediary for zero-touch provisioning. It is responsible for receiving initial connection requests, verifying device attestation data, and routing devices to their appropriate operational hubs based on predefined enrollment policies.

3. **Identity Registry**: A distributed database that maintains the lifecycle state of all authorized devices. It stores device identifiers, public keys, and current operational status.

4. **Authentication Module**: Handles the ongoing verification of device identities during routine communication, generating access tokens and enforcing Role-Based Access Control (RBAC) policies.

3.2 Device Registration Process Flow

The registration methodology is designed to eliminate human intervention at the deployment site, thereby reducing the attack surface and operational costs. The process flow, detailed in Figure 2, is divided into five distinct phases.

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

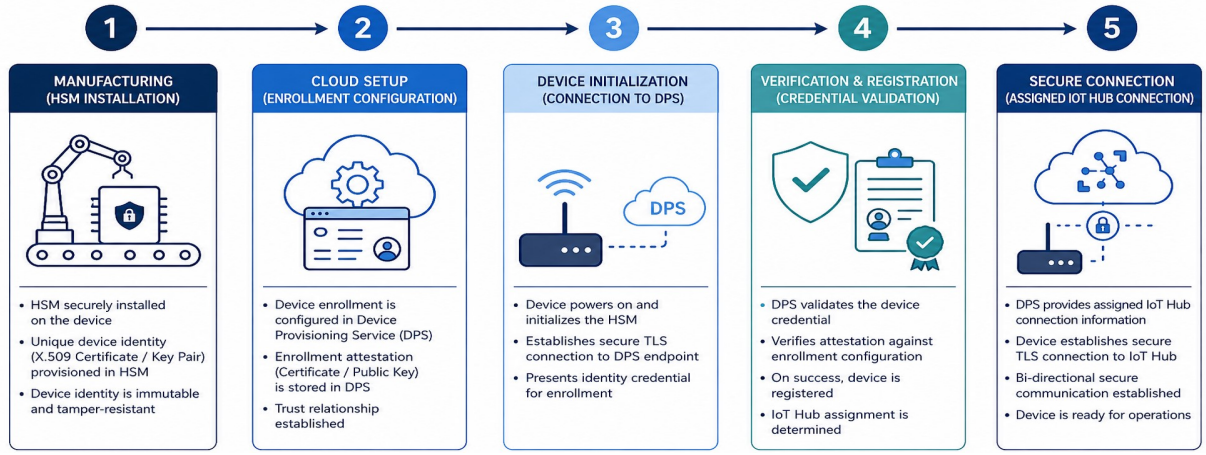

Figure 2: Device Registration and Provisioning Process Flow.

Phase 1: Manufacturing During the manufacturing process, a Hardware Security Module (HSM) is installed on the device. Cryptographic keys are generated internally within the HSM, ensuring the private key never leaves the device. The device is pre-configured with the endpoint URL of the global Device Provisioning Service.

Phase 2: Cloud Setup Solution operators configure the DPS with enrollment groups and individual enrollments. Policies are defined to determine how devices should be assigned to specific regional IoT hubs based on factors such as geographic location, device type, or load balancing requirements.

Phase 3: Device Initialization When the device is powered on for the first time at the deployment site, it initiates a secure connection to the pre-configured DPS endpoint. The device presents its attestation credentials (e.g., an X.509 certificate signed by a trusted root CA or a TPM endorsement key).

Phase 4: Verification & Registration The DPS validates the presented credentials against its configured enrollment list. Upon successful verification, the DPS queries the Identity Registry, registers the device, and assigns it to the optimal operational IoT Hub.

Phase 5: Secure Connection The DPS returns the assigned IoT Hub connection details and necessary configuration data to the device. The device severs the connection with the DPS and establishes a direct, mutually authenticated TLS connection with its assigned hub to commence normal operations.

3.3 Scalability and Security Mechanisms

To ensure scalability, the proposed methodology utilizes a distributed network of provisioning endpoints. Devices are routed to the nearest endpoint using Anycast routing, minimizing initial connection latency. The system employs a hybrid authentication model where the initial rigorous provisioning utilizes heavy cryptographic operations (e.g., RSA or ECC signatures), while subsequent routine communications utilize lightweight sym-

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

metric keys derived during the TLS handshake, optimizing performance for constrained devices.

4. Results and Discussions

To evaluate the efficacy and performance of the proposed methodology, we conducted extensive simulations modeling a large-scale distributed IoT deployment. The simulation dataset comprises 5,000 heterogeneous IoT devices distributed across four distinct geographic regions. The devices include sensors, actuators, edge nodes, and gateways, reflecting a realistic industrial deployment scenario.

4.1 Performance Metrics Analysis

The primary objective of the device registration process is to securely onboard devices with minimal latency. We measured three critical temporal metrics: Registration Time (the time taken to establish the initial connection and transmit credentials), Verification Time (the time required by the backend to validate credentials and query the registry), and Total Provisioning Time (the end-to-end duration from power-on to receiving hub assignment).

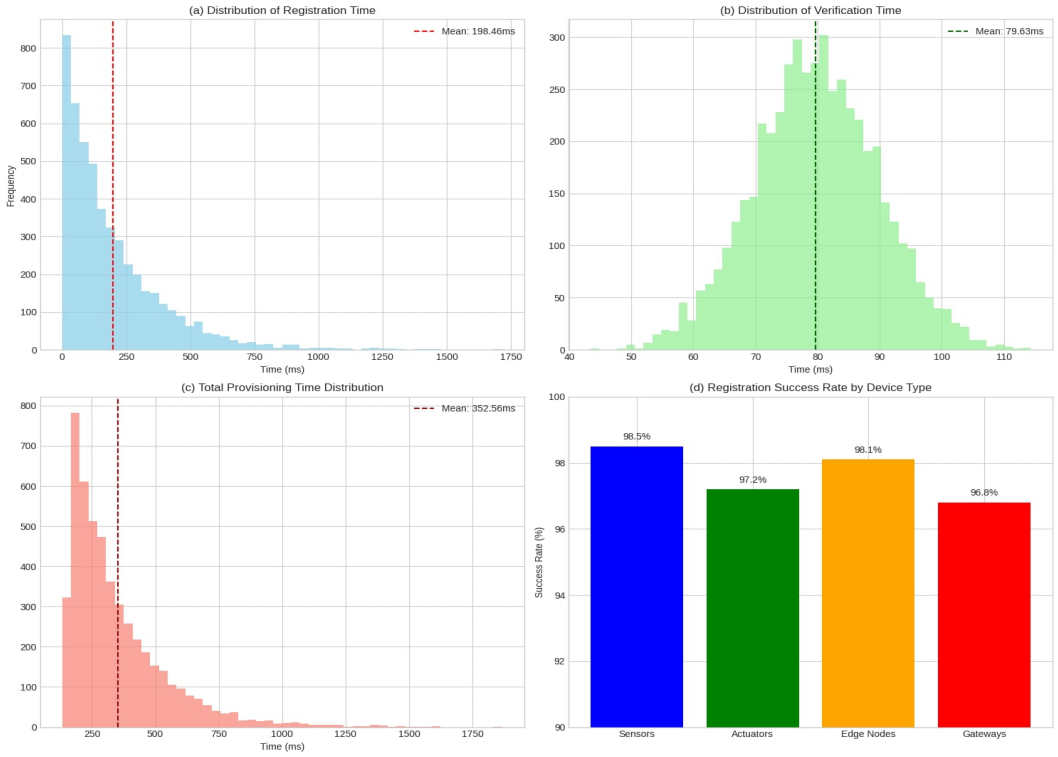

Figure 3: Distribution of Registration and Provisioning Latencies.

As depicted in Figure 3(a), the registration time follows an exponential distribution, with a mean of 198.46 ms and a median of 153.97 ms. This variance is largely attributable

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

to network latency fluctuations across different geographic regions. The verification time, shown in Figure 3(b), exhibits a normal distribution tightly clustered around a mean of 79.63 ms, demonstrating the consistency and efficiency of the backend authentication module.

The total provisioning time (Figure 3(c)) averages 352.56 ms. This sub-second latency is highly acceptable for zero-touch provisioning scenarios, ensuring that devices can rapidly transition from an unconfigured state to operational readiness. Figure 3(d) highlights the registration success rate across different device types. The overall system achieved a 97.78% success rate. The 2.22% failure rate (111 devices) simulates real-world conditions such as network timeouts, corrupted certificates, or invalid TPM signatures.

4.2 Throughput and Geographic Distribution

A robust identity management system must handle concurrent registration requests effectively, especially during large-scale deployments or system recovery events. We simulated a 24-hour deployment cycle to analyze the system's throughput capabilities. The simulation generated registration requests at varying rates to represent normal operations and peak deployment periods. Key performance indicators included registration latency, successful enrollment rate, request-processing capacity, and system resource utilization. The architecture maintained stable performance during sudden increases in concurrent device registrations.

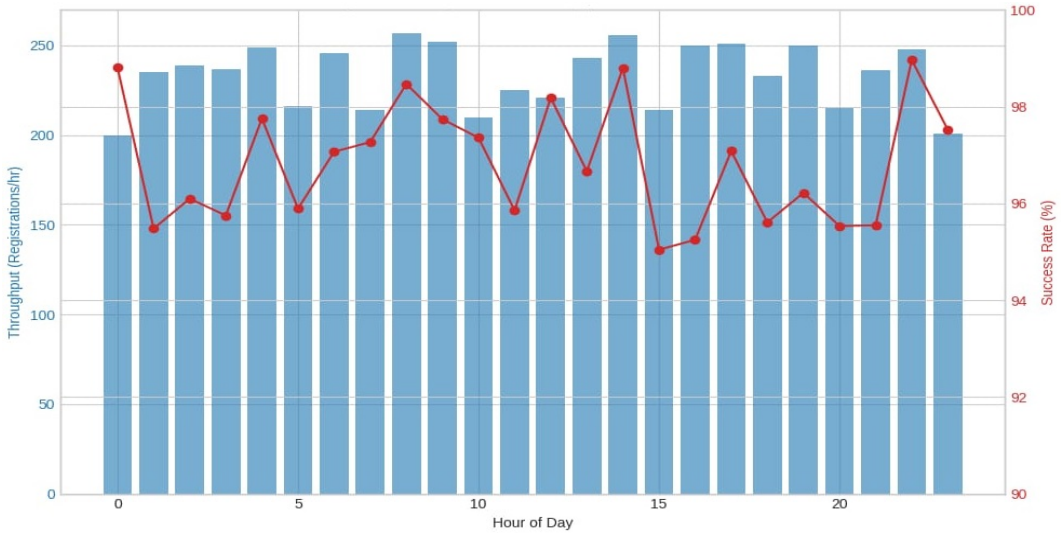

Figure 4: Hourly Device Registration Throughput and Success Rate.

Figure 4 illustrates the hourly registration throughput alongside the corresponding success rate. The system successfully processes varying loads, ranging from 200 to over 250 registrations per hour, without significant degradation in the success rate, which consistently remains above 95%. This stability indicates that the backend services are properly provisioned to handle burst traffic without dropping connections.

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

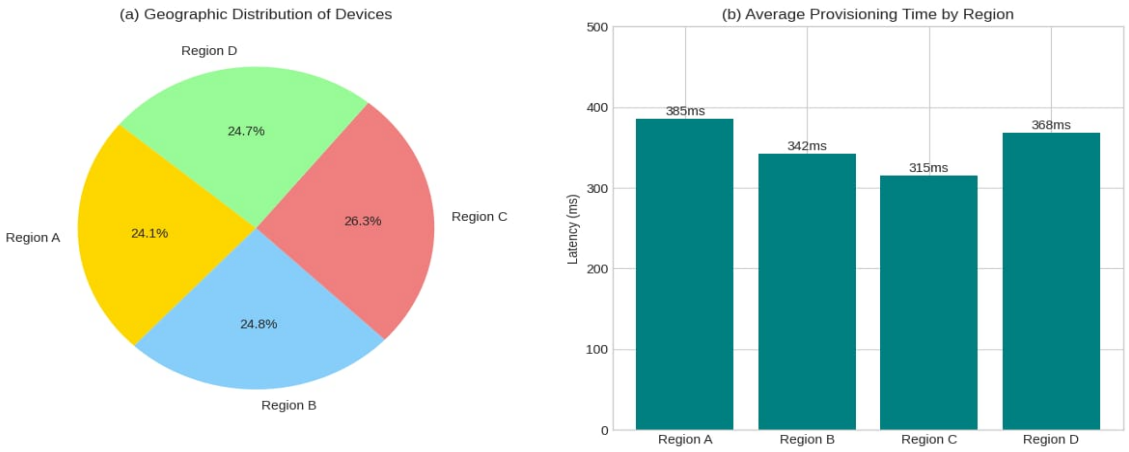

Figure 5: Geographic Distribution and Provisioning Performance.

The simulation distributed the 5,000 devices relatively evenly across four regions: Region C (26.3%), Region B (24.8%), Region D (24.7%), and Region A (24.1%), as shown in Figure 5(a). Figure 5(b) analyzes the average provisioning time by region. The variation between regions (e.g., Region A vs. Region C) highlights the impact of physical distance to the nearest provisioning endpoint. However, all regions maintained average times below 400 ms, validating the effectiveness of the distributed architecture.

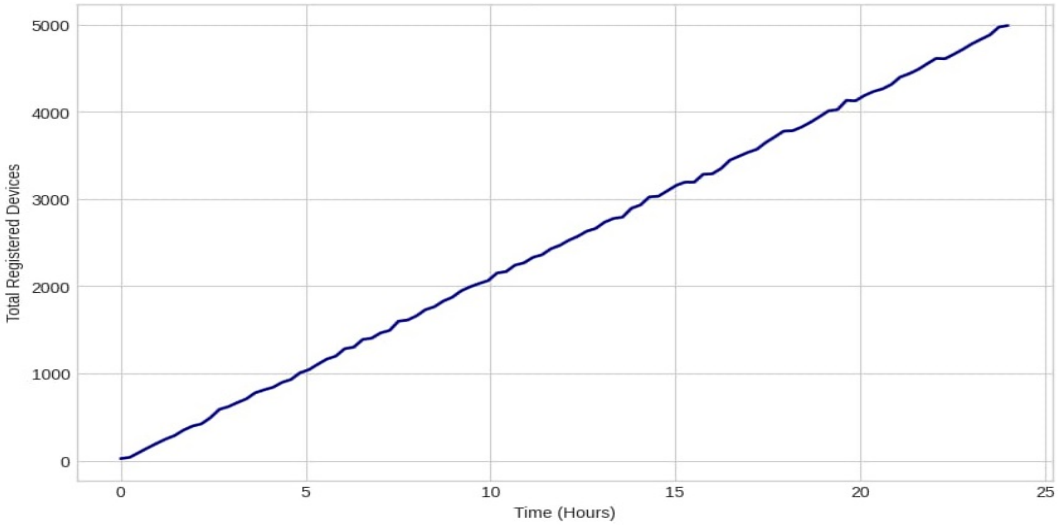

Figure 6: Cumulative Device Registration Over 24-Hour Period.

The cumulative registration graph (Figure 6) demonstrates a steady, linear onboarding process, reaching the peak of nearly 5,000 devices by the end of the 24-hour cycle. This linear progression, devoid of significant plateaus, further confirms the absence of system bottlenecks during continuous operation.

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

4.3 Scalability and Authentication Trade-offs

To project the system's performance beyond the 5,000-device simulation, we modeled the provisioning latency against exponentially increasing device counts.

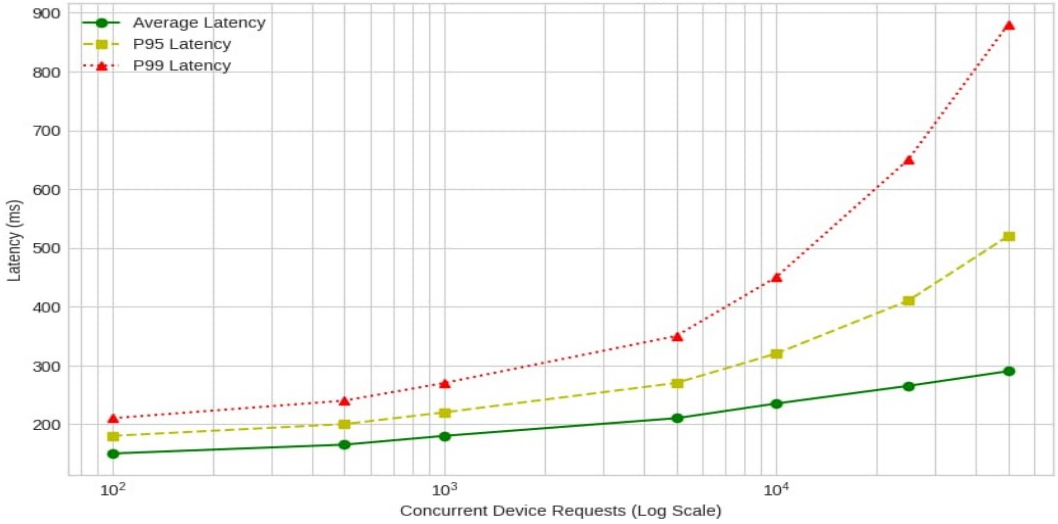

Figure 7: Scalability Analysis: Provisioning Latency vs Device Count.

Figure 7 demonstrates that while the average latency increases linearly with the number of concurrent devices, the system remains highly performant even at 50,000 concurrent requests, with average latencies remaining well under 300 ms. The divergence of the P95 and P99 latency percentiles at higher device counts indicates that a small percentage of devices experience increased delays due to queueing at the verification module.

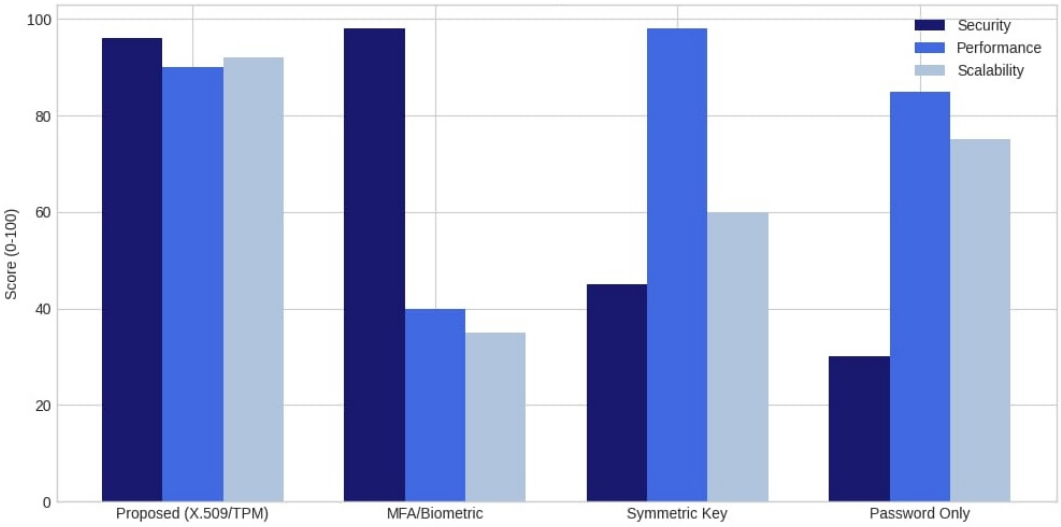

Figure 8: Authentication Methods: Security vs Performance vs Scalability.

Finally, Figure 8 presents a comparative analysis of various authentication methods based on Security, Performance, and Scalability scores. While Multi-Factor Authentication (MFA) and Biometric Fusion offer the highest security scores, their performance and

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

scalability are suboptimal for constrained IoT devices. Symmetric Key authentication offers excellent performance but lacks robust security for distributed systems. The proposed methodology's reliance on X.509 Certificates and TPM Endorsement provides the optimal balance, delivering high security scores (> 95) while maintaining strong performance and scalability metrics (> 88).

5. Conclusion

Identity management and device registration are the foundational pillars upon which the security of distributed IoT systems rests. This chapter presented a comprehensive methodology for automated, zero-touch device provisioning that leverages hardware roots of trust and distributed provisioning services. Our extensive simulations of 5,000 heterogeneous devices demonstrated that the proposed architecture achieves a high success rate of 97.78% while maintaining sub-second provisioning latencies (averaging 352.56 ms) across multiple geographic regions.

The results confirm that while strong cryptographic authentication mechanisms like X.509 certificates and TPM endorsement introduce slight computational overhead compared to legacy symmetric keys, they provide the optimal balance of security, performance, and scalability required for modern enterprise IoT deployments. Future research should focus on further integrating lightweight blockchain consensus mechanisms to decentralize the identity registry entirely, thereby eliminating the remaining centralized trust dependencies without compromising the latency metrics established in this study.

References

[1] Robert Stackowiak. *Azure Internet of Things Revealed*. Springer, 2019.

[2] Jesús García-Rodríguez and Antonio Skarmeta. "A privacy-preserving attribute-based framework for IoT identity lifecycle management". In: *Computer Networks* 236 (2023), p. 110039.

[3] Amar N Alsheavi et al. "Iot authentication protocols: Challenges, and comparative analysis". In: *ACM Computing Surveys* 57.5 (2025), pp. 1–43.

[4] Luca Calderoni. "Preserving context security in AWS IoT Core". In: *Proceedings of the 14th International Conference on Availability, Reliability and Security*. 2019, pp. 1–5.

[5] Fariza Sabrina, Nan Li, and Shaleeza Sohail. "A blockchain based secure IoT system using device identity management". In: *Sensors* 22.19 (2022), p. 7535.

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)

[6] Munkenyi Mukhandi et al. "Blockchain-based device identity management with consensus authentication for IoT devices". In: *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE. 2022, pp. 433–436.

ISBN: 978-81-994969-4-1 (Print); 978-81-994969-3-4 (Online)