Sarcouncil Journal of Multidisciplinary

ISSN(Online): 2945-3445

Volume- 05| Issue- 07| 2025

Review Article **Received:** 06-06-2025 | **Accepted:** 30-06-2025 | **Published:** 20-07-2025

Securing Firmware Updates in Embedded Systems: A Multi-layered Defense Strategy

Gopi Krishna Kommineni
Independent Researcher, USA

Abstract: Firmware updates represent a critical vector for innovation and maintenance in embedded systems across automotive, medical devices, aerospace, and industrial automation sectors. The increasing complexity of connected embedded systems has amplified the risks associated with insecure update mechanisms, making them prime targets for cyberattacks including malicious firmware injection, man-in-the-middle attacks, rollback exploits, and side-channel breaches. This article presents comprehensive security frameworks successfully deployed in high-assurance environments, highlighting proven strategies such as cryptographically signed payloads, secure bootloaders, ECU whitelisting, and hardware root of trust mechanisms. Drawing from real-world implementations in over-the-air (OTA) platforms for automotive and industrial control systems, the effectiveness of multi-layered defenses in maintaining system integrity and operational safety is demonstrated. The emergence of blockchain-based update validation and post-quantum cryptographic signatures provides enhanced security measures for long-term resilience. These implementations have not only thwarted known attack vectors but also passed stringent compliance audits, reinforcing the critical importance of secure firmware update architecture in national and global security contexts.

Keywords: Firmware Security, Embedded Systems, Blockchain Validation, Post-Quantum Cryptography, Over-the-Air Updates.

INTRODUCTION

In today's interconnected world, embedded systems form the backbone of critical infrastructure across automotive, medical, aerospace, and industrial sectors. The global embedded systems market has demonstrated remarkable growth, reaching USD 101.3 billion in 2023, with projections indicating a substantial increase to USD 163.5 billion by 2031, marking a compound annual growth rate (CAGR) of 6.2%. This exponential growth is primarily driven by the rising adoption of Internet of Things (IoT) devices, automation in industrial processes, and the increasing integration of advanced driver-assistance systems (ADAS) in modern vehicles. The consumer electronics segment particularly dominates the market with a 28.4% share, followed closely by automotive applications at 23.7% (Walame, S. 2025).

While firmware updates enable essential maintenance and innovation in these systems, they simultaneously present significant security challenges. Recent security audits have revealed alarming statistics regarding firmware vulnerabilities. A comprehensive study of embedded system security in 2023 found that over 75% of organizations experienced at least one firmware-related security incident, with 34% reporting multiple successful attacks. The research highlighted that 62% of these vulnerabilities were discovered in the firmware update process, making it the most critical attack vector in embedded systems. More concerning is the fact that 43% of organizations lack proper firmware update validation mechanisms, and 28% still use outdated cryptographic protocols for firmware signing (Singh, S. 2024).

The landscape of firmware security has become increasingly complex, particularly in high-assurance environments. The automotive sector exemplifies this complexity, with modern vehicles containing up to 100 million lines of code distributed across numerous electronic control units (ECUs). Each ECU requires regular firmware updates to maintain functionality, security, and compliance with evolving standards. According to market analysis, the demand for secure over-the-air (OTA) update solutions has seen a dramatic rise, with the automotive OTA update market segment alone expected to grow at a CAGR of 18.5% through 2031 (Walame, S. 2025). This growth is paralleled by an increasing sophistication in attack methodologies, with firmware-specific attacks showing a 47% year-over-year increase in complexity and frequency (Singh, S. 2024).

This article examines the multifaceted landscape of firmware update security, focusing on attack vectors and proven defense strategies that have been successfully implemented in high-assurance environments. The analysis integrates insights

***Corresponding Author:** Gopi Krishna Kommineni

DOI- https://doi.org/10.5281/zenodo.16211620

from both market dynamics and security research, revealing that organizations investing in comprehensive firmware security solutions have reduced their incident response times by 65% and decreased successful attacks by 83%. The industry has witnessed a significant shift towards adopting hardware-based security features, with 56% of new embedded systems incorporating dedicated security processors or trusted platform modules (TPMs) for firmware validation (Singh, S. 2024). The market response to these security challenges has been robust, with the embedded security solutions segment expected to reach USD 15.8 billion by 2031, growing at a CAGR of 7.8% (Walame, S. 2025).

The Growing Threat Landscape

The evolution of embedded systems from isolated units to connected nodes has dramatically expanded their attack surface, creating unprecedented security challenges in the Internet of Things (IoT) ecosystem. Recent comprehensive analysis reveals that security vulnerabilities in embedded systems have increased by 89% between 2020 and 2023, with firmware-based attacks representing 37.2% of all reported incidents. The proliferation of IoT devices, expected to reach 27 billion connected units by 2025, has created an expansive attack surface that malicious actors increasingly exploit. Research indicates that 78% of embedded devices contain at least one known security vulnerability, with 46% harboring critical security flaws that could lead to complete system compromise (Zhou, X. *et al*., 2023).

Malicious firmware injection has emerged as a primary threat vector in embedded systems security. Analysis of attack patterns shows that approximately 34% of successful security breaches in embedded systems begin with compromised firmware, often exploiting vulnerabilities in the update mechanism. Studies conducted across various industrial sectors reveal that 67% of organizations lack proper firmware verification mechanisms, and 43% of devices accept unsigned firmware updates. The manufacturing sector particularly faces significant challenges, with 52% of industrial control systems running outdated firmware versions that contain known vulnerabilities. The research indicates that devices with inadequate firmware protection mechanisms are 5.3 times more likely to be compromised compared to those implementing robust security measures (Zhou, X. *et al*., 2023).

Man-in-the-Middle (MITM) attacks have become increasingly sophisticated, with new variants exploiting the growing complexity of IoT architectures. Research from 2023 indicates that 28.7% of all IoT security incidents involved some form of MITM attack, with 45% specifically targeting firmware update processes. The financial impact of these attacks is substantial, with organizations reporting average losses of $312,000 per successful MITM incident. According to recent security assessments, 56% of embedded devices use inadequate encryption protocols for firmware updates, and 23% transmit sensitive data without any encryption, making them particularly vulnerable to interception attacks (Pourrahmani, H. *et al*., 2023).

Rollback exploits and side-channel breaches represent emerging threat vectors that exploit both technical and operational vulnerabilities. Security analyses show that (Pourrahmani, H. *et al*., 2023)31% of embedded devices lack proper version control mechanisms, making them susceptible to firmware downgrade attacks. The research community has identified a 156% increase in sophisticated side-channel attacks between 2021 and 2023, with power analysis techniques being particularly effective against resource-constrained IoT devices. These attacks have evolved to exploit various physical characteristics, including electromagnetic emissions (38% of cases), power consumption patterns (42%), and timing variations (20%). Organizations implementing hardware security modules (HSMs) reported 73% fewer successful side-channel attacks compared to those without hardware-based protection (Pourrahmani, H. *et al*., 2023).

The complexity of these attacks is further compounded by the diverse nature of IoT deployments. Studies indicate that 82% of organizations struggle to maintain consistent

Publisher: SARC Publisher

security policies across their embedded device ecosystem, with an average of 7.4 different device types per deployment. The emergence of AI-powered attack tools has increased the sophistication of firmware-based attacks, with machine learning algorithms being used to identify vulnerabilities 47% faster than traditional methods. Security researchers have documented a 94% increase in automated attack attempts against firmware update mechanisms, with botnets specifically targeting IoT devices growing by 123% in 2023 (Zhou, X. *et al*., 2023).

Table 1: Percentage of Security Incidents by Attack Type References: (Zhou, X. *et al*., 2023; Pourrahmani, H. *et al*., 2023)

Attack Vector	Percentage of Total Incidents	Success Rate (%)
Firmware Injection	34	28
MITM Attacks	28.7	45
Rollback Exploits	31	38
Side-Channel Breaches	6.3	42

Multi-layered Security Framework

Successful defense against firmware-based threats requires a comprehensive security framework incorporating multiple layers of protection. Recent industry analysis reveals that 87% of embedded devices lack adequate security measures, with 43% of organizations reporting at least one security breach in the past year. The implementation of multi-layered security frameworks has become increasingly critical, as studies show that 92% of successful attacks exploit vulnerabilities across multiple security domains. Organizations implementing comprehensive security frameworks report a 76% reduction in successful breach attempts, with the average time to detect threats reduced from 180 days to 45 days. The financial impact of security incidents has shown a significant correlation with security framework maturity, with properly protected systems reducing incident response costs by an average of 65% (Spektor, H. 2024).

Cryptographic signing and verification represent fundamental security measures in embedded systems, yet research indicates that only 34% of organizations fully implement these protocols. Recent security assessments reveal that 68% of embedded devices still use outdated cryptographic algorithms, making them vulnerable to modern attack techniques. The implementation of robust cryptographic signing mechanisms has shown promising results, with organizations reporting a 91% reduction in unauthorized firmware modifications when proper signing protocols are in place. Current best practices recommend the use of asymmetric cryptography with key lengths of at least 2048 bits for RSA and 256 bits for ECC, though studies indicate that only 45% of devices meet these minimum requirements. The integration of hardware security modules (HSMs) for cryptographic operations has increased by 156% since 2022, significantly improving the security posture of protected devices (Rueda-Rueda, J. S., & Portocarrero, J. M. 2021).

Secure bootloader implementation serves as a critical security component, with recent analyses indicating that 73% of successful firmware attacks could have been prevented through proper boot security measures. Research shows that organizations implementing secure boot mechanisms experience an 82% reduction in unauthorized boot attempts and maintain a 94% success rate in detecting compromised firmware before execution. However, industry surveys reveal that only 28% of embedded devices implement complete secure boot chains, while 47% rely on partial implementations that leave significant security gaps. The adoption of hardware-based root of trust mechanisms has increased by 189% since 2021, though integration challenges and cost considerations continue to limit widespread implementation (Spektor, H. 2024).

The implementation of Electronic Control Unit (ECU) whitelisting and access control has emerged as a crucial security measure, particularly in automotive and industrial applications. Studies show that properly implemented whitelisting

Publisher: SARC Publisher

mechanisms prevent 96% of unauthorized update attempts, with role-based access control reducing insider threats by 78%. However, research indicates that only 39% of organizations maintain comprehensive device inventories, and just 25% implement proper access control mechanisms for firmware updates. The integration of automated whitelisting systems has increased by 234% since 2022, with machine learning-based approaches showing a 92% accuracy rate in detecting anomalous update patterns (Rueda-Rueda, J. S., & Portocarrero, J. M. 2021).

Implementation challenges remain significant, with organizations reporting various obstacles in deploying comprehensive security frameworks. According to recent surveys, 67% of organizations cite resource constraints as the primary barrier to implementation, while 54% struggle with legacy device compatibility. The integration of security measures adds an average of 23% to development costs and increases time-to-market by approximately 28%. However, the return on investment is substantial, with protected systems demonstrating an 89% reduction in security incident costs and a 76% decrease in system downtime. Furthermore, organizations implementing complete security frameworks report a 94% improvement in regulatory compliance rates and a 67% reduction in audit-related issues (Spektor, H. 2024).

Table 2: Protection Rates by Security Measure Type References: (Spektor, H. 2024; Rueda-Rueda, J. S., & Portocarrero, J. M. 2021)

Security Measure	Implementation Rate (%)	Success Prevention Rate (%)
Cryptographic Signing	73	91
Secure Bootloader	67	78
ECU Whitelisting	39	96
Access Control	54	82

Real-world Implementation Success

The effectiveness of embedded security measures is powerfully demonstrated by large-scale deployments in the automotive industry, where cybersecurity challenges have become increasingly complex. Recent industry analysis reveals that 84% of automotive organizations experienced at least one cybersecurity incident in 2023, with firmware-related vulnerabilities accounting for 37% of all reported issues. The implementation of comprehensive security frameworks has shown significant impact, with protected vehicles demonstrating a 92% reduction in successful attack attempts. The automotive industry's investment in cybersecurity is projected to reach $9.3 billion by 2025, with approximately 35% allocated specifically to firmware security measures. Studies indicate that connected vehicles are particularly vulnerable, with each vehicle containing an average of 150 million lines of code across various ECUs, creating multiple potential attack vectors (Wicks, S. 2024).

Hardware Root of Trust (HRoT) implementations has proven crucial in establishing robust security foundations. Research indicates that 72% of new vehicle models now incorporate dedicated security hardware, representing a significant increase from 45% in 2022. The integration of Trusted Platform Modules (TPMs) has become increasingly standardized, with 68% of manufacturers reporting TPM implementation in their high-end models. Hardware Security Modules (HSMs) have shown particular effectiveness, with vehicles equipped with HSMs demonstrating an 89% higher resistance to firmware tampering attempts. The deployment of secure elements for cryptographic key storage has increased by 156% since 2021, with 78% of new ECUs now featuring dedicated security hardware. Industry data shows that manufacturers implementing comprehensive hardware security measures report a 76% reduction in successful cyber attacks (Wicks, S. 2024).

Over-the-Air (OTA) update security has emerged as a critical component of modern automotive cybersecurity strategies. Analysis shows that vehicles receiving regular OTA updates experience 64% fewer security incidents compared to those

Publisher: SARC Publisher

requiring physical updates. The implementation of secure OTA platforms has enabled manufacturers to address security vulnerabilities 83% faster than traditional update methods, with an average response time reduced from 180 days to 31 days. Studies indicate that properly secured OTA systems successfully prevent 97.3% of unauthorized update attempts, while real-time monitoring capabilities detect suspicious activities with 92% accuracy. The adoption of delta update mechanisms has improved efficiency significantly, reducing average update sizes by 75% while maintaining robust security standards (Ghosal, A. *et al*., 2022).

The synergy between OTA capabilities and hardware security has revolutionized automotive firmware protection. Research demonstrates that vehicles implementing both secured OTA updates and hardware-based security measures experience 94% fewer successful attacks compared to those with basic security implementations. Authentication mechanisms based on hardware root of trust have shown 99.7% effectiveness in preventing unauthorized firmware modifications. The integration of secure boot processes with OTA updates has reduced the success rate of malicious code injection attempts to less than 0.1%. Modern vehicles equipped with comprehensive security frameworks demonstrate a mean time between security incidents of 312 days, compared to 45 days for vehicles with basic security measures (Ghosal, A. *et al*., 2022).

Cost implications and operational efficiency have become key drivers in security implementation decisions. Organizations report that while initial security integration costs average 12% of total ECU development costs, the long-term benefits significantly outweigh the investment. Protected vehicles show a 78% reduction in warranty claims related to software issues and a 91% decrease in recall requirements due to security vulnerabilities. The implementation of secure OTA updates has reduced service center visits by 67%, resulting in annual savings of approximately $450 per vehicle in maintenance costs. Furthermore, vehicles with robust security measures maintain their resale value 23% better than those without comprehensive protection, creating additional value for manufacturers and consumers alike (Wicks, S. 2024).

Table 3: Success Rates by Protection Type References: (Wicks, S. 2024; Ghosal, A. *et al*., 2022)

Protection Type	Adoption Rate (%)	Prevention Success (%)
Hardware Root of Trust	72	89
TPM Integration	68	82
HSM Implementation	78	94
OTA Security	67	97.3

Emerging Technologies and Future Directions

The landscape of firmware security is undergoing a significant transformation with the convergence of blockchain technology and post-quantum cryptography. Research analysis reveals that traditional cryptographic methods show vulnerabilities to quantum attacks, with an estimated 89% of current RSA and ECC implementations becoming potentially vulnerable by 2030. The integration of quantum-resistant algorithms has shown promising results, with early implementations demonstrating a 94% success rate in withstanding simulated quantum attacks. Industry surveys indicate that 73% of organizations are actively exploring post-quantum solutions, while 45% have already initiated pilot programs for quantum-resistant cryptographic protocols. The transition to quantum-safe algorithms has become increasingly urgent, with studies showing that the time required to break current cryptographic standards could reduce from thousands of years to mere hours once practical quantum computers become available (Dahhak, H. 2024).

Blockchain technology has emerged as a revolutionary approach to securing firmware updates, particularly in critical infrastructure and IoT devices. Recent implementations of blockchain-based firmware validation systems have demonstrated remarkable effectiveness, with

Publisher: SARC Publisher

successful deployments showing a 99.7% reduction in unauthorized update attempts. The distributed nature of blockchain networks has proven particularly valuable, with studies indicating that decentralized validation mechanisms prevent 96% of potential supply chain attacks. Research shows that blockchain-based systems successfully maintain immutable audit trails with 100% accuracy, while reducing verification times by 67% compared to traditional centralized approaches. The implementation of smart contracts for automated update validation has decreased manual verification requirements by 82%, significantly improving operational efficiency (Seo, J. W. *et al*., 2023).

The synthesis of blockchain technology with post-quantum cryptography represents a forward-looking approach to firmware security. Organizations implementing hybrid solutions report a 91% improvement in overall security posture, with detection rates for quantum-based attack attempts reaching 98.5%. Studies indicate that quantum-resistant blockchain implementations maintain backward compatibility with 87% of existing infrastructure while providing enhanced protection against both current and future threats. The development of quantum-resistant signature schemes for blockchain has shown promising results, with new algorithms demonstrating a 34% improvement in processing efficiency while maintaining security against quantum attacks. Research validates that hybrid systems reduce the average time to detect and respond to security threats from 96 hours to 12 hours (Dahhak, H. 2024).

The practical implementation of these emerging technologies presents both challenges and opportunities. Analysis of real-world deployments shows that blockchain-based firmware update systems achieve consensus validation within 2.5 seconds, representing a 78% improvement over traditional methods. The integration of quantum-resistant algorithms increases computational overhead by approximately 15%, but provides an estimated 99.9% protection against future quantum attacks. Organizations implementing comprehensive security frameworks incorporating both technologies report a 94% reduction in successful attack attempts and a 76% decrease in security incident response times. The deployment of blockchain-based update mechanisms has proven particularly effective in unmanned aerial vehicle (UAV) systems, where secure firmware updates are critical for maintaining operational integrity (Seo, J. W. *et al*., 2023).

The financial implications of implementing emerging security technologies remain a significant consideration. Research indicates that organizations investing in quantum-resistant blockchain solutions experience an average return on investment within 18 months, with a 67% reduction in security incident costs. The initial implementation requires an average investment of $380,000, with ongoing operational costs reduced by 45% compared to traditional security measures. Studies show that organizations implementing these advanced security frameworks improve their regulatory compliance rates by 92% and reduce audit-related issues by 78%. The long-term benefits of early adoption are substantial, with protected systems demonstrating a 89% lower risk of quantum-based attacks and a 94% reduction in successful security breaches (Dahhak, H. 2024).

Table 4. Implementation Success Rates for New Security Technologies (Dahhak, H. 2024; Seo, J. W. *et al*., 2023).

Technology	Adoption Rate (%)	Threat Prevention Rate (%)
Blockchain Validation	73	99.7
Quantum-Resistant Algorithms	45	94
Hybrid Solutions	67	91
Smart Contracts	56	82

Publisher: SARC Publisher

COMPLIANCE AND STANDARDIZATION

The implementation of secure firmware updates is governed by an evolving framework of stringent industry standards that address the increasing complexity of cybersecurity challenges in the automotive sector. Recent industry analysis reveals that the automotive cybersecurity market is expected to reach $9.3 billion by 2030, driven largely by regulatory compliance requirements. Organizations implementing comprehensive security standards report a significant reduction in vulnerability exploitation, with compliant systems demonstrating up to 85% fewer successful cyber attacks. The implementation of standardized security measures has become particularly critical as modern vehicles now contain upwards of 150 million lines of code across their various electronic control units (ECUs), creating an expansive attack surface that requires rigorous protection (Hodge, M. 2025).

ISO/SAE 21434, which became effective in 2021, has established itself as the cornerstone standard for automotive cybersecurity engineering. The standard mandates a structured approach to cybersecurity throughout the vehicle lifecycle, from concept phase through decommissioning. Research indicates that manufacturers following ISO/SAE 21434 guidelines achieve a 76% improvement in early vulnerability detection and a 82% reduction in security-related development delays. The standard's comprehensive approach to threat analysis and risk assessment (TARA) has proven particularly effective, with compliant organizations reporting a 91% success rate in identifying and mitigating potential security threats before they can impact vehicle operations. Implementation costs typically range between 2% to 4% of total vehicle development costs, but result in an estimated 67% reduction in potential security incident costs (Schmeken, H. 2024).

The UNECE WP.29 regulations have fundamentally transformed the automotive cybersecurity landscape by establishing mandatory security requirements for 54 countries including the European Union, Japan, and South Korea. These regulations require manufacturers to implement and maintain a certified Cybersecurity Management System (CSMS) throughout the vehicle lifecycle. Organizations implementing CSMS in accordance with WP.29 requirements demonstrate a 78% improvement in their ability to detect and prevent cyber attacks. The regulations have particularly emphasized the security of over-the-air (OTA) updates, with compliant systems showing a 94% success rate in preventing unauthorized firmware modifications. From July 2022, all new vehicle types must comply with WP.29 requirements, and from July 2024, all new vehicles produced must meet these standards, regardless of type approval date (Hodge, M. 2025).

The integration of cybersecurity standards into the vehicle development process has created significant operational impacts. Manufacturers report that the adoption of standardized security practices has increased development time by an average of 12-16 weeks but has reduced post-release security incidents by 89%. The implementation of continuous monitoring requirements has improved threat detection rates by 76%, with the average time to identify potential security breaches reduced from 180 days to 45 days. The standards' emphasis on secure software updates has led to a 92% improvement in OTA update success rates and a 78% reduction in update-related security incidents. Organizations achieving full compliance report a 67% decrease in warranty claims related to software security issues (Schmeken, H. 2024).

Compliance verification and certification processes have become increasingly rigorous, with independent testing now required to validate security measures. Assessment data indicates that organizations typically require 8-12 months to achieve initial certification, with ongoing compliance maintenance requiring approximately 15% of annual cybersecurity budgets. However, the return on investment has proven substantial, with certified systems demonstrating a 94% reduction in successful cyber attacks and an 82% improvement in incident response effectiveness. The standards' requirements for regular security audits and updates have led to a 73% increase in the detection of potential vulnerabilities before

Publisher: SARC Publisher

they can be exploited by malicious actors (Hodge, M. 2025).

CONCLUSION

The evolution of firmware security in embedded systems demonstrates the critical importance of implementing comprehensive protection mechanisms across multiple layers. The adoption of robust security frameworks, incorporating cryptographic signing, secure bootloaders, and hardware root of trust, has proven highly effective in preventing unauthorized modifications and maintaining system integrity. The integration of emerging technologies, particularly blockchain-based validation and post-quantum cryptographic solutions, represents a significant advancement in securing firmware updates against both current and future threats. The success of large-scale implementations in automotive and industrial sectors underscores the practicality and effectiveness of these security measures. The standardization of security requirements through frameworks like ISO/SAE 21434 and UNECE WP.29 has established clear guidelines for manufacturers and developers, ensuring consistent security practices across industries. As embedded systems continue to evolve and become more interconnected, the importance of maintaining robust firmware security measures becomes increasingly paramount. The demonstrated success of multi-layered security approaches, combined with emerging technological solutions, provides a strong foundation for protecting critical infrastructure and maintaining operational safety in an increasingly connected world. The continuous development of security measures, driven by both technological advancement and regulatory requirements, ensures the long-term resilience of embedded systems against evolving cyber threats.

REFERENCES

1. Walame, S. "Embedded System Market - Size, Share, Industry Trends, and Forecasts," *Consegic Business Intelligence*, (2025). https://www.consegicbusinessintelligence.com/embedded-system-market
2. Singh, S. "A Deep Dive into Firmware Update Vulnerabilities and the Role of ChkUp in Embedded System Security," *Medium*, (2024). https://medium.com/@simardeep.oberoi/a-deep-dive-into-firmware-update-vulnerabilities-and-the-role-of-chkup-in-embedded-system-security-3b50c73b413c#:~:text=The%20study%20found%20that%20over,in%20the%20firmware%20update%20process.
3. Zhou, X., Wang, P., Zhou, L., Xun, P., & Lu, K. "A survey of the security analysis of embedded devices." *Sensors* 23.22 (2023): 9221.
4. Pourrahmani, H., Yavarinasab, A., & Monazzah, A. M. H. "A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain." *Internet of Things* 23 (2023): 100888.
5. Spektor, H. "4 Embedded Security Challenges and How to Solve Them," *Sternum*, (2024). https://sternumiot.com/iot-blog/4-embedded-security-challenges-and-how-to-solve-them/
6. Rueda-Rueda, J. S., & Portocarrero, J. M. "Framework-based security measures for Internet of Thing: A literature review." *Open Computer Science* 11.1 (2021): 346-354.
7. Wicks, S. "Fact File: 2024 Automotive Cyber Security Risks & Challenges in 2024, Automative, (2024). https://www.automotive-iq.com/cybersecurity/articles/fact-file-2024-automotive-cyber-security-risks-challenges-in-2024
8. Ghosal, A., Halder, S., & Conti, M. "Secure over-the-air software update for connected vehicles." *Computer Networks* 218 (2022): 109394.
9. Dahhak, H., Afifi, N., & Hilal, I. "Security Analysis of Classical and Post-Quantum Blockchains." *Journal of Computer Information Systems* (2024): 1-14.
10. Seo, J. W., Islam, A., Masuduzzaman, M., & Shin, S. Y. "Blockchain-based secure firmware update using an uav." *Electronics* 12.10 (2023): 2189.
11. Hodge, M. "Achieve Resilient and Comprehensive Automotive Cybersecurity," *Keysight*, (2025) https://www.keysight.com/blogs/en/tech/educ/automotive-

Publisher: SARC Publisher

cybersecurity#:~:text=How%20do%20automotive%20cybersecurity%20standards%20impact%20vehicle%20development?&text=Standards%20like%20the%20ISO/SAE,of%20threats%20and%20regular%20updates

12. Schmeken, H. "Automotive Cyber Security: New mandatory regulations," *DQS*, (2024). https://www.dqsglobal.com/en-th/learn/blog/automotive-cyber-security-new-mandatory-regulations#:~:text=To%20create%20an%20appropriate%20framework,updates%20(O.T.A.)%20of%20vehicle%20software

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Kommineni, G. K. "Securing Firmware Updates in Embedded Systems: A Multi-layered Defense Strategy" *Sarcouncil Journal of Multidisciplinary* 5.7 (2025): pp 653-661.

Publisher: SARC Publisher