PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 07 • June 2026

TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Silicon Sovereignty: Securing Pakistan's Embedded Future in an Era of Quantum Threats and Invisible Attacks

With billions of embedded devices shaping our world today, "invisibility" in the form of firmware has become the holy grail of cybercriminals. This paper provides a detailed analysis of the role played by the secure booting process, hardware security measures, and adoption of quantum-safe encryption methods in making cybersecurity a prerequisite for emerging technologies in Pakistan.

By **Ishmal Yasir** | University of Agriculture, Faisalabad | Published: June, 2026
ishmalyasir456@gmail.com | Position: Student (Computer Science)

Introduction

The environment of technology around the globe is witnessing a revolution that is subtle yet drastic. This is not only about computers and phones but also about the existence of "embedded intelligence" all around us. The meters measuring energy levels in Lahore, the controllers regulating the production process in Faisalabad, and the machines performing tests in Karachi hospitals are all examples of embedded devices. Currently, there are more than 21 billion IoT-enabled devices, and the growth rate is 14% per year.,

This rapid development has generated an equally large-scale threat. Traditionally, cybersecurity dealt with the software layer. But now, this struggle has moved down to the silicon level. Cybercriminals have understood that the software which directs how the hardware should function, called firmware, can be an ideal target. If hackers succeed in taking control of the firmware of any device, they take complete control over the machine.

This is an extremely pertinent issue when considering the current tech revolution in Pakistan, whereby our agritech startups are already installing thousands of soil sensors and our fintech companies have started rolling out PoS terminals. This is because the security of the aforementioned hardware products forms the backbone of the very business of the startup firms.,

Firmware security and Secure Boot, which are the tools needed for this unseen warfare, have ceased to be luxuries that are only afforded by expensive military equipment, but necessities for all "secure by design" hardware. When firmware is secure, it breaks the attack chain, thus protecting everything built upon it.

> ***"Hardware without Secure Boot in this digital age is akin to building a castle with no entrance. No matter how high your software walls may be, the enemy is already inside."***

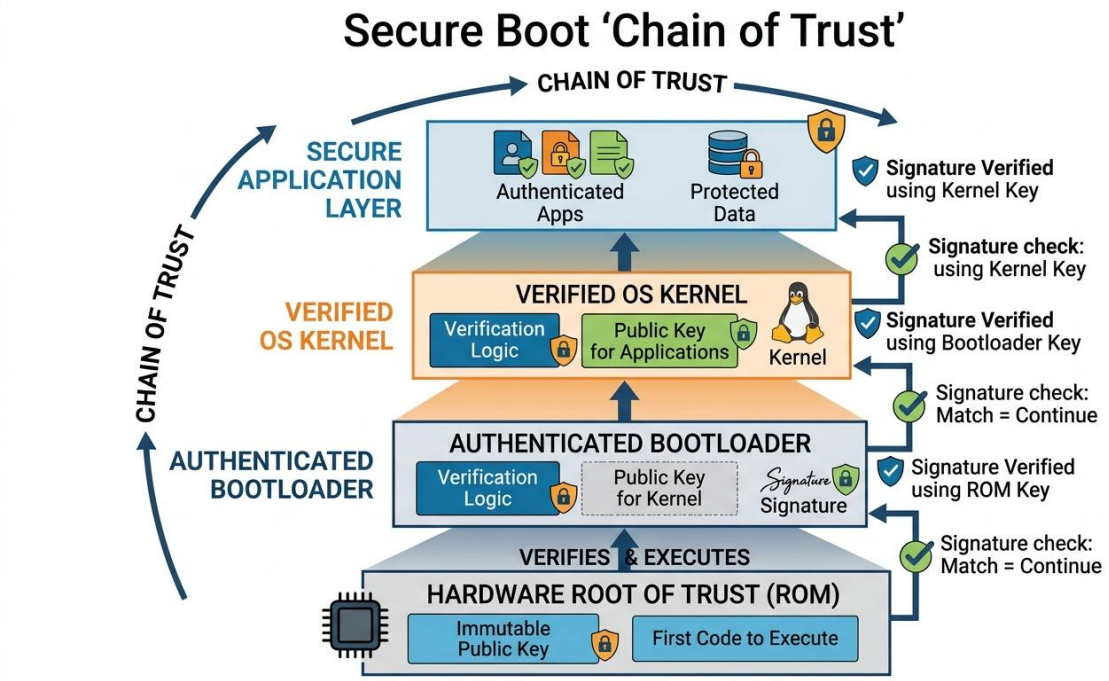
Technology Overview

In order to fully comprehend the idea of secure boot, it is necessary to think about booting an embedded device in analogy to the process of accessing a castle via its drawbridge. Secure boot can be seen as the guardian at the entrance, who checks each piece of software for

proper authorization. From a technical point of view, it means that the device verifies whether the firmware it is running was authorized and signed by the manufacturer.

The trick that makes it possible is based on cryptography. Namely, the manufacturer signs the firmware with their private key. The device itself has a small area of memory where the public key is stored. Then, the device compares the hash of the firmware with the signed version. If they match, the software is considered authentic and not modified. However, even if a single bit of code changes, the verification will fail, resulting in inability to proceed with the boot sequence.,

Besides booting, the firmware protection provides the "Chain of Trust." Namely, the initial bootloader – the so-called "Root of Trust" – authenticates the secondary bootloader, which verifies the OS kernel, which in turn authenticates the application.



Among others are:

***Secure Update**: The update itself should be digitally signed in order to prevent "malware injection," meaning that an attacker will inject malware into what looks like a legitimate update file.*

***Encryption**: To encrypt the firmware in order for the attacker, in case they obtain the firmware files from the server, to be unable to access its content in any way.*

Anti-Rollback Protections: Utilizing hardware counters to ensure that an attacker cannot force a device to go "backward" to a vulnerable firmware version.

Real-life examples reveal how critical the situation can become. As recently as 2017, the FDA had to recall more than half a million pacemakers due to potential threats from hackers who could mess with the device's pulse. The well-known Stuxnet worm was able to cause physical damage to the industrial controllers (PLCs) through compromising their firmware, forcing them to run at extremely high speeds.

Key Findings & Impact

This study of embedded security from 2020 to 2026 has uncovered vital key findings that can have a significant impact in Pakistan.

Impact on Local Startups: The first problem faced by the local startup community is the "security-cost tradeoff". Adding complete hardware-based security solutions to the design could hike the BOM cost of devices

by anything between $1 and $15. But it emerges that the "SRAM PUF" approach enables "high security at zero additional silicon area," which would be perfect for low-cost devices. Startups cannot limit themselves to software-based security any longer because more than 32% of all firmware images today have more than 10 vulnerabilities.

Security and Performance in Industry: In the case of the industry, "secure lifecycle management" is the important point. The device used in a textile mill today could keep running for well over a decade. It will need "cryptographic agility" to allow for changes as new types of threats emerge., The data available on performance suggests that today's modular approaches enable security updates of a 1.2MB firmware image within 1.73 seconds.

Government & Policy: With Pakistan adopting international guidelines such as the EU Cyber Resilience Act, we must advocate for "PSA Certification" by our regulators. This multi-tier certification ensures a "minimum viable security":

Tier 1: Reviewing documentation for consumer IoT.

Tier 2: Lab tests from an independent facility for medical devices and home products.

Tier 3: Resistance to physical attacks for critical infrastructures and defense purposes.

What's Next?

The trend for future embedded security will involve a "Zero Trust" paradigm for embedded hardware where the embedded device does not trust itself or its environment but continually evaluates its status through anomaly detection via artificial intelligence and self-attestation.,,

Upcoming Trends:

- **Use of AI in Hardware Security:** Even though AI-based machine learning can assist hardware security systems in detecting any unusual behavior in power consumption patterns, it can also be used offensively to extract patterns in the side channel information much faster than humans can.
- **Use of Post-Quantum Hybrid Signatures:** Devices are expected to have hybrid signatures for at least a couple of years until post-quantum standards fully develop and include a combination of classical elliptic curve cryptography and Dilithium-based PQC.,
- **Formal Verification:** It is becoming more common to see the use of "formally verified" security primitives. Formal verification uses mathematics to prove that a component of hardware or software does not contain any certain categories of vulnerabilities.,

Roadblocks Ahead: Despite the advancements, there are several obstacles that still need to be overcome. "Developer friction" is among them; many engineers do not specialize in the field of cybersecurity, and configuring such things as TEEs and Secure Boot processes can become a challenge for them. Automated tooling and code partitioning are necessary to allow these complex systems to be used even by an average developer.

About the Author

Author Name is Ishmal Yasir. Author has a strong interest in cybersecurity and emerging technologies. With experience in building modern web applications and researching advanced cryptographic systems, she focuses on bridging practical development with future-ready security solutions. She can be reached at ishmalyasir456@gmail.com.

Keywords: Cybersecurity, IoT, Embedded Systems, Secure Boot, Firmware Protection, Root of Trust, Side-Channel Attacks, Post-Quantum Cryptography, Pakistan Tech.

References

[1] A. Kia, A. W. Storey, and M. Imtiaz, "Advanced Hardware Security on Embedded Processors: A 2026 Systematic Review," *Electronics*, vol. 15, no. 5, p. 1135, 2026.

[2] S. Jones, C. Tremlet, and M. Jackson, "The Fundamentals of Secure Boot and Secure Download: How to Protect Firmware and Data Within Embedded Devices," *New-TechEurope*, Jun. 30, 2017.

[3] S. Falas, C. Konstantinou, and M. K. Michael, "A Modular End-to-End Framework for Secure Firmware Updates on Embedded Systems," *arXiv:2007.09071 [cs.CR]*, Oct. 2021.

[4] A. Dave, N. Banerjee, and C. Patel, "FVCARE: Formal Verification of Security Primitives in Resilient Embedded SoCs," *arXiv:2304.11489 [cs.CR]*, Apr. 2023.

[5] M. Fagan, K. N. Megas, K. Scarfone, and M. Smith, "Foundational Cybersecurity Activities for IoT Device Manufacturers," *NIST Interagency Report NISTIR 8259*, 2020.

[6] M. Pursche et al., "SoK: The Engineer's Guide to Post-Quantum Cryptography for Embedded Devices," *IACR Cryptology ePrint Archive*, Paper 2024/1345, 2024.

[7] Intrinsic ID, "Intrinsic ID Protects 500,000,000 Devices Globally," *EEJournal Industry News*, 2023.