STM JOURNALS

International Journal of
VLSI Circuit Design & Technology

ISSN: 3139-356X
Volume 4, Issue 1, 2026
January–June
DOI (Journal): 10.37591/IJVCDT

https://journals.stmjournals.com/ijvcdt

Review IJVCDT

An Overview of VLSI-Based Hardware Security in IoT Node

Kazi Kutubuddin Sayyad Liyakat[1], Heena Shaikh[2,*], Kosgiker G.M.[3]

Abstract

In the coming era, security will not be a feature we add *to an Internet of Things (IoT) device; it will be a property* inherent *to its transistor-level design. By encoding security into the very large-scale integration (VLSI) architecture, we move away from the fragile "software-only" paradigm and toward a future where the identity of the device is as immutable as the laws of physics. The rapid proliferation of IoT devices has transformed global infrastructure, yet it has simultaneously exposed a critical vulnerability: the hardware layer. As IoT nodes are frequently deployed in physically insecure, remote, or hostile environments, they are uniquely susceptible to side-channel attacks, fault injections, and invasive reverse engineering. Traditional software-based security measures often prove insufficient due to their high computational overhead and vulnerability to kernel-level exploits. This paper explores the paradigm shift toward VLSI-based hardware security as the "Root of Trust" for IoT ecosystems. We examine the implementation of physical unclonable functions (PUFs), hardware-based true random number generators (TRNGs), and logic locking techniques embedded directly into the silicon fabric. By integrating security primitives at the architectural level, we demonstrate a methodology for achieving high-assurance cryptographic protection with minimal area, power, and latency constraints. The findings underscore that hardware-centric security is not merely an auxiliary feature but a fundamental requirement for the sustainable and secure evolution of the IoT landscape.*

Keywords: VLSI, IoT, security, hardware security, IoT node security

INTRODUCTION

In the sprawling landscape of the Internet of Things (IoT), we are witnessing the democratization of intelligence. From smart pacemakers and industrial sensors to autonomous drones, the "edge" is where data breathes. However, this ubiquity comes with a chilling paradox: the more we connect, the more we expose ourselves [1–4].

***Author for Correspondence**
Heena Shaikh
E-mail: 98shaikhheena@gmail.com

[1]Professor and Head, Department of Electronics and Telecommunication Engineering, Brahmdevdada Mane Institute of Technology, Solapur, Maharashtra, India
[2]Assistance Professor, Department of Electronics and Telecommunication Engineering, Brahmdevdada Mane Institute of Technology, Solapur, Maharashtra, India.
[3]Associate Professor, Department of Electronics and Telecommunication Engineering, Brahmdevdada Mane Institute of Technology, Solapur, Maharashtra, India.

Received Date: March 16, 2026
Accepted Date: May 22, 2026
Published Date: May 26, 2026

Citation: Kazi Kutubuddin Sayyad Liyakat, Heena Shaikh, Kosgiker G.M. An Overview of VLSI-Based Hardware Security in IoT Node. International Journal of VLSI Circuit Design & Technology. 2026; 4(1): 52–58p.

When a sensor node, which is a tiny piece of silicon, is deployed in an untrusted environment, it becomes a vulnerable frontier. Traditional software-based security, which relies on firewalls and OS-level encryption, is often too heavy for these resource-constrained devices. If the "brain" of the node is compromised, the software is easily bypassed. Therefore, the solution must be etched in stone—or, more accurately, in silicon.

This is imperative for VLSI-based hardware security. By shifting security from the volatile layer of code to the immutable layer of transistors, we create a "Silicon Shield" that is as robust as the architecture. At the heart of hardware security lies the physical unclonable function (PUF). Just as no

© STM Journals 2026. All Rights Reserved

two humans share the same thumbprint, no two integrated circuits are identical at the microscopic level. Variations in doping, lithography, and etch rates during the manufacturing process create unique random delays in transistors [5–10].

By exploiting these variations, a PUF generates a unique "private key" that exists only when the device is powered on. It is never stored in memory, making it immune to physical probing and reverse engineering. When the device is off, the secret vanishes, rendering the node a "blank slate" for any attacker attempting to extract keys through side-channel analysis.

An IoT node running an encryption algorithm emits subtle physical signatures, such as power consumption spikes, electromagnetic emanations, and timing fluctuations. A sophisticated attacker can monitor these "side channels" to deduce a secret key mathematically. VLSI design offers a proactive defense against such attacks. Through Logic obfuscation and Asynchronous Logic Design**,** engineers can mask these emissions. By inserting "dummy" gate switching or utilizing dual-rail logic (where every operation is balanced by an inverse operation), the power profile becomes a flat and indistinguishable line of noise. The attacker is left staring at a screen of static, unable to distinguish the secret work from the noise [11–14].

The most insidious threat is the Hardware Trojan (HT), a malicious modification inserted during the third-party fabrication process. A few rogue transistors can sit dormant for years, only to activate and leak data when they detect a specific sequence of sensor values.

To address this, we are moving toward Trust-Verification Architectures. Recent advancements in VLSI design have allowed for the development of "Self-Checking Circuits." These are integrated watchdogs that perform real-time verification of the chip netlist, ensuring that the actual silicon behaves exactly as dictated by the mathematical model. It is a form of industrial immunity—the chip essentially "senses" when it is tampered with.

The future of VLSI security in IoT nodes is not just about preventing theft; it is about hardware resilience. We are moving toward a paradigm where circuits can "self-destruct" their sensitive data if physical tampering is detected (e.g., laser-cut circuitry or focused ion beam intervention) and where lightweight cryptographic cores are implemented at the hardware level to ensure that encryption adds negligible latency to the node's primary function [15–20].

In the future, security will not be a feature that we *add* to an IoT device; it will be a property *inherent* in its transistor-level design. By encoding security into the VLSI architecture, we move away from the fragile "software-only" paradigm and toward a future in which the identity of the device is as immutable as the laws of physics.

VLSI-based hardware security in IoT nodes focuses on embedding security mechanisms directly into integrated circuits (ICs) to protect against physical and cyberattacks. As IoT devices are often resource-constrained with limited power and processing capabilities, hardware-level security provides an efficient, lightweight, and high-speed alternative to traditional software-based security.

Key aspects of VLSI hardware security for IoT nodes include:

Core Security Mechanisms

- *Physically unclonable functions:* These leverage unique physical variations in silicon during fabrication to create a "fingerprint" for a chip, allowing secure key generation and authentication without storing secrets in memory.
- *Lightweight cryptography accelerators:* Dedicated hardware engines for algorithms such as AES, a lightweight block cipher, or SIMON/SPECK provide fast encryption and decryption with

© STM Journals 2026. All Rights Reserved

low power consumption, tailored for constrained devices.
- *Hardware root of trust (HRoT):* A secure core within the system on a chip (SoC) ensures that only trusted code boots, protecting against malware.
- *Tamper-resistant designs:* Techniques such as metal shielding, active shielding, and sensors are implemented to detect and respond to physical probing or reverse engineering.

Common Attacks and Countermeasures
- *Hardware Trojans:* Malicious modifications during design/manufacturing are countered by logic testing and design for security.
- *Physical probing/cloning:* Protected by PUFs, tamper detection circuits, and secure packaging techniques.
- *Data eavesdropping:* Secured using hardware-based encryption accelerators that maintain high-speed communication without adding significant latency.

Implementation Approaches
- *FPGA-based security:* Used for prototyping and low-to-medium volumes, enabling reconfigurable security algorithms.
- *ASIC (Application-specific integrated circuit):* Used for high-volume, cost-sensitive IoT products, where custom security logic is hardened directly into the silicon.

FRAMEWORK

A comprehensive framework for VLSI-based hardware security in IoT nodes focuses on providing a "root of trust" at the chip level, as traditional software security is inadequate for resource-constrained edge devices.

This framework typically integrates lightweight cryptographic accelerators, PUFs for authentication, and secure storage to ensure confidentiality, integrity, and authenticity of the data.

Key Components of the VLSI Security Framework as shown in Figure 1:
- *Physical unclonable functions:* These utilize unique, uncontrollable manufacturing variations within silicon (such as transistor threshold voltages or propagation delays) to generate device-specific, immutable identifiers and keys. Common types include arbiter PUFs and ring oscillator (RO) PUFs.
- *Lightweight cryptographic cores:* Implement ciphers designed for low-power constraints, such as authenticated encryption algorithms (for authenticated encryption), AES-GCM, or PRESENT, rather than high-overhead conventional algorithms.
- *Hardware security modules (HSM) / trusted platform modules (TPM):* These modules provide dedicated hardware for secure key storage and cryptographic operations, acting as secure vaults.
- *Side-channel attack (SCA) countermeasures:* include noise generators, power-aware masking, and dual-rail logic to prevent attacks that monitor power consumption, timing, or electromagnetic emissions to leak secret keys.
- *Hardware trojan detection:* Incorporates techniques such as built-in self-test (BIST) or side-channel analysis to verify that the IC has not been tampered with during manufacturing.

Operational Workflow (3-Stage Approach)
1. *Generation and initialization:* A Secure PUF (SP-PUF) architecture is introduced to generate a unique digital fingerprint, which is encrypted and stored at the foundry or during device provisioning.
2. *Obfuscation/locking:* Logic obfuscation techniques are applied to hide the functional relationship between inputs and outputs, making it difficult for attackers to reverse-engineer the chip, even if they have the netlist.
3. *Authentication protocol:* A challenge-response pair mechanism is used, where the node and server authenticate each other using the PUF response without directly storing the secret key in memory.

© STM Journals 2026. All Rights Reserved

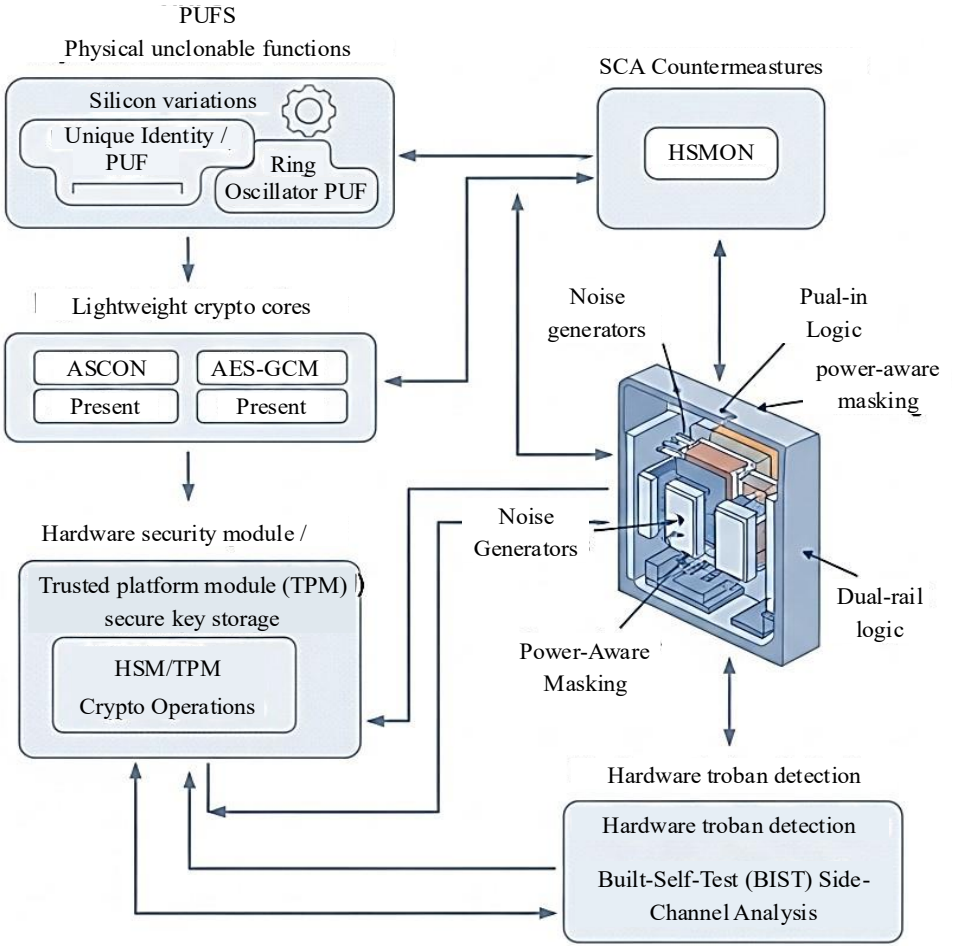


Figure 1. Framework.

Design Considerations (Power, Performance, and Area (PPA) Factors)

- *Low power:* IoT nodes often operate on batteries or energy harvesting; thus, security modules must minimize dynamic and static power consumption (e.g., using 7 nm nodes or SLVT MOSFETs).
- *Small area:* The silicon footprint must be minimal, often utilizing optimized look-up table (LUT) approaches.
- *High performance:* Cryptographic latency must be low enough for real-time applications.

Common Evaluation Tools

- *Simulation:* Xilinx Vivado, Mentor Graphics Modelsim, Cadence Virtuoso.
- *Metrics analysis:* Throughput, gate count, energy/bit, latency.

RESULTS AND DISCUSSION

The results for VLSI-based hardware security in IoT nodes focus on balancing robust, tamper-resistant protection with extremely low power consumption, minimal area, and high throughput. Key performance parameters show that dedicated hardware acceleration, such as lightweight cryptography, outperforms software-based security, with expected reductions in energy consumption of up to 44% and significant area optimization.

Key performance parameters and expected results.

- *Area overhead (area efficiency):* Optimized designs (e.g., using 65 nm, 45 nm, or 28 nm complementary metal–oxide–semiconductor (CMOS) aim for a small footprint, often limiting security modules to (< 10-15%) of the total IoT node area.

© STM Journals 2026. All Rights Reserved

Table 1. Summary of expected results by security mechanism.

Security mechanism	Typical expected outcome	Key metrics
PUF (key gen/auth)	Unique, reliable, tamper-resistant digital fingerprint	<0.5% BER, 99.8% uniqueness
Lightweight crypto (LWC)	High-speed encryption with minimal energy, e.g., PRESENT, ANU	Area (mu m^2), Power (mu W), Throughput
Logic Locking/obfuscation	Prevents IP theft and reverse engineering	Min. latency penalty, high security level
Secure boot/root of trust	Ensures secure, uncompromised boot-up process	Boot time, Tamper detection

IP: Intellectual Property

- *Power consumption (energy efficiency):* Sub-microwatt (mu W) to low-milliwatt (mW) levels are standard, with advanced designs achieving high energy efficiency (e.g., 0.057 fJ/b).
- *Performance/throughput:* High-speed data encryption with low latency is expected, often exceeding Gbps throughput for advanced encryption standards (e.g., AES-128/256 and PRESENT).
- *Reliability and security:* PUFs typically achieve a uniqueness of ~50% (ideal) and reliability over 99.5% (error rates (< 0.5%)).
- *Side-channel attack resistance:* Improved resistance to power analysis and differential power analysis (DPA) attacks via hardware countermeasures.

Table 1 shows the results of the security mechanism based on VLSI-based IoT node security.

Expected Performance Trends

1. *Reduced latency:* Optimized VLSI algorithms allow for faster encryption and decryption than traditional software approaches.
2. *Low-power operation:* Techniques such as dynamic voltage scaling (DVS) and subthreshold operations help maintain high-efficiency energy usage.
3. *Hardware Trojan detection:* High detection probability in both pre-silicon and post-silicon phases.

CONCLUSION

The convergence of VLSI design and cybersecurity represents the most viable defense strategy against sophisticated threats facing modern IoT nodes. As demonstrated throughout this study, reliance on software obfuscation is no longer a sustainable strategy for resource-constrained devices. By shifting the security burden from firmware to the hardware substrate, we create a defensive perimeter that is inherently resilient to remote software exploitation.

The integration of advanced VLSI primitives, specifically PUFs for device authentication and logic obfuscation for intellectual property protection, enables a “Zero Trust” architecture at the chip level. Although challenges remain regarding the scaling of these security features within nanometer-scale processes (such as reliability under environmental thermal fluctuations), advancements in CMOS-compatible security logic offer a clear path forward. Ultimately, the future of a secure IoT depends on our ability to embed integrity into the transistors that power it. Hardware security is the bedrock upon which the next generation of trustworthy, connected technology must be built, ensuring that the devices of tomorrow are as secure as they are interconnected.

REFERENCES

1. Pasaya A, Hadia S, Bhatt K. Bio-inspired power optimization strategies for low-power VLSI in IoT and wearable devices: A comprehensive review. Discover Electronics. 2026;3(1):53. doi:10.1007/s44291-026-00189-9.
2. Yuan JS, Lin J, Alasad Q, Taheri S. Ultra-low-power design and hardware security using emerging

© STM Journals 2026. All Rights Reserved

technologies for Internet of Things. Electronics (Basel). 2017;6(3):67. doi:10.3390/electronics6030067.
3. Jadhav M, Nerkar PM. FPGA-based finger vein recognition system for personal verification. Int J Eng Res Gen Sci. 2015;3:382-388.
4. Nerkar PM, Kazi Kutubuddin Sayyad Liyakat, Dhaware BU, Kazi Sayyad Shaikh Liyakat. Predictive data analytics framework based on heart healthcare system (HHS) using machine learning. J Adv Zool. 2023;44(Spec Iss 2):3673-3686.
5. Deepa S, Kumar SP, Arun V, Lalidesh J. The role of VLSI in next-generation IoT systems. In: Kumar A, Tripathi SL, editors. Smart Chips for Smart Devices: VLSI Design for Next-Generation IoT Solutions. Hoboken (NJ): John Wiley & Sons; 2026. p. 249-267. doi:10.1002/9781394335831.ch13.
6. Poswal R, Deshwal M, Johar AK. Review of VLSI architecture of cryptography algorithm for IoT security. In: Kumar A, Mozar S, editors. Proceedings of the 6th International Conference on Communications and Cyber Physical Engineering (ICCCE 2024). Lecture Notes in Electrical Engineering. Vol. 1096. Singapore: Springer; 2024. Chapter 9. doi:10.1007/978-981-99-7137-4_9.
7. Sidhu S, Mohd BJ, Hayajneh T. Hardware security in IoT devices with emphasis on hardware trojans. J Sens Actuator Netw. 2019;8(3):42. doi:10.3390/jsan8030042.
8. Akter S, Khalil K, Bayoumi M. A survey on hardware security: Current trends and challenges. IEEE Access. 2023;11:77543-77565. doi:10.1109/ACCESS.2023.3288696.
9. Japa A, Majumder MK, Sahoo SK, Vaddi R, Kaushik BK. Hardware security exploiting post-CMOS devices: Fundamental device characteristics, state-of-the-art countermeasures, challenges and roadmap. IEEE Circuits Syst Mag. 2021;21(3):4-30. doi:10.1109/MCAS.2021.3092532.
10. Knechtel J. Hardware security for and beyond CMOS technology: An overview on fundamentals, applications, and challenges. Proceedings of the 2020 International Symposium on Physical Design (ISPD '20); 2020 Sep 20-23; Taipei, Taiwan. New York (NY): Association for Computing Machinery; 2020. p. 75-86. doi:10.1145/3372780.3378175.
11. Rose GS. Introduction: Overview of VLSI, nanoelectronics, and hardware security. In: Tehranipoor M, Forte D, Rose GS, Bhunia S, editors. Security Opportunities in Nano Devices and Emerging Technologies. Boca Raton (FL): CRC Press; 2017. p. 3-18. doi:10.1201/9781315265056-1.
12. SenGupta A, Kundu S. Guest editorial: Securing IoT hardware: Threat models and reliable, low-power design solutions. IEEE Trans Very Large Scale Integr (VLSI) Syst. 2017;25(12):3265-3267. doi:10.1109/TVLSI.2017.2762398.
13. Halak B, Zwolinski M, Mispan MS. Overview of PUF-based hardware security solutions for the Internet of Things. 2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS), Abu Dhabi, United Arab Emirates. 2016. p. 1-4. doi:10.1109/MWSCAS.2016.7870046.
14. Hu W, Chang CH, SenGupta A, Bhunia S, Kastner R, Li H. An overview of hardware security and trust: Threats, countermeasures, and design tools. IEEE Trans Comput Aided Des Integr Circuits Syst. 2021;40(6):1010-1038. doi:10.1109/TCAD.2020.3047976.
15. Rajendran S, Syed A, Lourde RM. Security of an IoT network: A VLSI point of view. In: Ranganathan G, Chen J, Rocha Á, editors. Inventive Communication and Computational Technologies: Proceedings of ICICCT 2019. Singapore: Springer Singapore; 2020. p. 789-798. doi:10.1007/978-981-15-0146-3_75.
16. Tudosa I, Picariello F, Balestrieri E, De Vito L, Lamonaca F. Hardware security in the IoT era: The role of measurements and instrumentation. 2019 II Workshop on Metrology for Industry 4.0 and IoT (MetroInd4.0&IoT), Naples, Italy. 2019. p. 285-290. doi:10.1109/METROI4.2019.8792895.
17. Knechtel J. Hardware security for and beyond CMOS technology. Proceedings of the 2021 International Symposium on Physical Design (ISPD '21); 2021 Mar 22-24; Virtual Event, USA. New York (NY): Association for Computing Machinery; 2021. p. 115-126. doi:10.1145/3439706.3446902.
18. Dofe J, Frey J, Yu Q. Hardware security assurance in emerging IoT applications. 2016 IEEE International Symposium on Circuits and Systems (ISCAS), Montreal, QC, Canada. 2016. p. 2050-

© STM Journals 2026. All Rights Reserved

2053. doi:10.1109/ISCAS.2016.7538981.
19. Malarkodi K. VLSI circuit architectures for scalable IoT implementations. 2024 9th International Conference on Communication and Electronics Systems (ICCES); 2024 Dec 16-18; Coimbatore, India. 2024. p. 127-133. doi:10.1109/ICCES63552.2024.10859955.
20. Divyanshu D, Kumar R, Khan D, Amara S, Massoud Y. Logic locking using emerging 2T/3T magnetic tunnel junctions for hardware security. IEEE Access. 2022;10:102386-102395. doi:10.1109/ACCESS.2022.3208650.

© STM Journals 2026. All Rights Reserved