Journal of People and Worldviews (JPW)
Maiden Edition, Volume 1, Number 1 (Part 2)
Review Article
Open Access

Hardware-Based Security Mechanisms for IoT Devices in Emerging Economies

Abstract

Underneath smart systems in homes, farms, industries, and public services lies the security of Internet-connected devices, which depends on the small pieces of hardware embedded within them. For emerging economies, IoT technologies are expanding rapidly, but resource and infrastructure constraints persist. To secure these hardware foundations becomes not just a technical concern, but a developmental one. This study examined how hardware-based security techniques currently defend IoT devices and how far these mechanisms stretch when applied in environments with limited budgets, inconsistent standards, and evolving cybersecurity capacity. Employing a systematic literature review approach, recent scholarly works were gathered, screened, and synthesized to capture contemporary viewpoints on secure boot processes, cryptographic chips, trusted execution environments, physically unclonable functions, and related hardware-anchored defenses. The findings showed that hardware-rooted trust models offer durable resistance to physical tampering and unauthorized access. They also require investment, specialized supply chains, stable power supply and skilled talent, which can be uneven or emerge in developing regions. The study concluded that strengthening hardware security in IoT systems for emerging economies will demand not only technology but also strategic, inclusive innovation that prioritizes cost realities, infrastructure maturity, and the need for scalable, context-sensitive protection.

Keywords: Internet Security, Hardware, Emerging Economies, Device Protection, Power Supply

Adeogun Abiola Adekunle
Department of Computer Science
Federal College of Agriculture,
Ishiagu, Ebonyi State
Mobile: 08059773976
ORCID ID: 0009-0004-6241-1048

Omini Moses Omori
Department of Computer Science
Independent Researcher
Mobile: 08148255474
Email: ominiriches@gmail.com
ORCID ID: 0009-0001-9040-3457

Ayanniran Felix Oluwaseun
Department of Computer Science Technology
Federal College of Agriculture,
Ishiagu, Ebonyi State
Mobile: +2348163353134
Email:
ayanniran.felix@fcaishiagu.edu.ng
ORCID ID: 0009-0003-5424-7391.

Corresponding Author's Email:
olowoo4real2023@yahoo.com

Date Received: 10th March, 2026

Date Accepted: 25th March, 2026

Doi: https://doi.org/10.5281/zenodo.19385245

1. Introduction

The proliferation of Internet-connected devices in homes, farms, industries, and public services is reshaping how emerging economies engage with the digital infrastructure. The mainstay of this transformation is not only the network layer but also the fixed hardware within each device. Hardware elements such as microcontrollers, microprocessors, system-on-chip (SoCs), and field-programable gate arrays (FPGAs) are used for processing and form part of the brain of IoT systems. (Williams, 2022) In resource-constrained settings, where the power supply is inconsistent and supply

chains may be fragile, the reliability of these hardware components becomes a critical issue. Failures in hardware-anchored security can undermine the trustworthiness of the entire IoT ecosystem.

Hardware-based security mechanisms such as secure boot, cryptographic modules, trusted execution environments, and physically unclonable functions offer a durable approach to resisting physical tampering and unauthorized access. For example, Chatterjee (2025) observed that hardware security has become one such layer that focuses on safeguarding various hardware components and embedded systems against physical and side-channel attacks. These mechanisms are especially relevant in emerging economies where IoT devices may be deployed in unattended or less-secure environments. However, the gap between mainstream research and practice in such environments remains significant.

Emerging economies confront infrastructure, budgetary and skills constraints in ways that differ significantly from those of high-income economies. A recent study examining IoT acquisition in emerging economies points out how factors such as unreliable power supply, limited regulatory frameworks and scarcity of technical talent hamper deployment (Tondro, Jahanbakht, & Ozay, 2025). When hardware security requires specialized supply chains or stable environmental conditions, the promise of the IoT can be compromised. Furthermore, the transfer of hardware-anchored security technologies to low-resource settings is seldom seamless as the design often neglects local realities.

Rapid IoT adoption, rising hardware-rooted security threats, and context-specific constraints in emerging economies are imperative to the study's focus. First, the device numbers are growing, raising the attack surface. Williams (2022) reported a growing number of studies emphasizing IoT security threats and solutions. Second, hardware-rooted trust models are gaining traction as a more robust solution compared to purely software-based defenses. Lastly, emerging economies may not reap the full benefits of those models without adaptation to local budget, infrastructure and capacity realities. This suggests a developmental dimension to the hardware security in IoT systems.

The current study examines how hardware-based security techniques defend IoT devices and how far these mechanisms stretch when applied in environments with limited budgets, inconsistent standards, and evolving cybersecurity capacity. The analysis proceeds by systematically surveying recent scholarly works, screening and synthesizing findings on secure boot processes, cryptographic chips, trusted execution environments, physically unclonable functions and related hardware-anchored defenses. The study also uncovers evidence that while global research has progressed strongly, direct technology transfer to resource-constrained regions is uneven.

Objectives of the Study

Citation: Adekunle, Adeogun A. ; Omori, Omini M. & Oluwaseun, Ayanniran F. "Hardware-Based Security Mechanisms for IoT Devices in Emerging Economies". *Journal of People and Worldviews (JPW),* 2026: pp115-126.

The study's objectives are to:

i. Identify and analyze contemporary hardware-based security mechanisms used in IoT systems, including secure boot processes, cryptographic modules, trusted execution environments, and physically unclonable functions.
ii. Assess the practical applicability and performance of these mechanisms in emerging economies.
iii. Examine the key infrastructural, economic, and technical constraints that affect the deployment of hardware-anchored IoT security in low-resource environments.
iv. Explore how global hardware security technologies can be adapted, simplified, or redesigned to suit the realities of emerging economies.

Research Question

i. What contemporary hardware-based security mechanisms are used to protect IoT devices, and what functions do they perform in safeguarding device integrity and trust?
ii. How effectively do these hardware-based mechanisms operate when applied in emerging economies where budgets, standards and technical capacity may be uneven?
iii. What infrastructural, economic, and skills-related constraints limit the deployment and performance of hardware-anchored IoT security in resource-constrained settings?
iv. In what ways can existing global hardware security technologies be adapted or redesigned to align with the specific realities of developing regions?

Statement of the Problem

The expansion of IoT devices globally brings a dramatically increased attack surface as the precipitate volume of IoT devices enormously increases potential vulnerabilities, which means that hardware vulnerabilities cannot be ignored (Laghari *et al.*, 2024). Simply deploying hardware-rooted security mechanisms under the assumptions of well-resourced settings introduces a mismatch when applied in emerging economies. In many developing regions, IoT devices are introduced into contexts characterized by infrequent power supply, weak regulatory oversight, fragmented supply chains, and limited technical skills. For example, a recent investigation found that businesses acquiring IoT technology in emerging markets face infrastructure constraints, regulatory frameworks, and the importance of strategic alliances as major hurdles. (Tondro, Jahanbakht & Ozay, 2025). When high-end hardware security features require constant power, secure installation environments, and specialized maintenance, the conditions in emerging economies threaten their effective deployment.

Additionally, hardware-based security mechanisms are often developed with the assumptions of strong manufacturing quality, stable logistics, and regular firmware updates.

However, research shows that IoT devices are often deployed in unattended or physically exposed locations in resource-limited regions, increasing the chance of tampering or side-channel attack. This means that hardware threats may be amplified in situations where environmental protections are weaker. While hardware-rooted trust models promise robust resistance to physical tampering, their cost, supply chain complexity, and need for skilled talent can render them impractical in low-resource settings. In short, the technology transfer from high-resource to low-resource settings is rarely seamless.

Literature Review

Recent research positions hardware as the anchor point for securing IoT systems. Hardware-based identity mechanisms provide stronger resistance to device impersonation and cloning attacks because they rely on physical properties rather than software constructs. This establishes the hardware as not only a performance component but also a foundational trust layer. Shamsoshoara *et al*. (2020) buttressed this status by noting that the hardware roots of trust create a reliable security baseline for authentication and attestation in distributed environments. Therefore, the literature converges around the idea that robust IoT security begins with reliable embedded hardware.

Ling *et al*. (2021) explained that secure boot protects IoT platforms by ensuring that only verified and authorized firmware images are executed during startup. This function blocks persistent malware and firmware tampering. Trusted execution environments extend this defense by isolating sensitive operations inside dedicated secure zones. Trusted environments built on TPM 2.0 support attestation protocols that strengthen device-level trustworthiness, especially in distributed IoT deployments. However, these mechanisms depend on stable provisioning processes and reliable update channels, which are often inconsistent in emerging economies.

Cryptographic modules embedded in IoT devices also allow for secure key storage and on-chip cryptographic operations that reduce the exposure to memory-based exploits. Modern secure elements serve as isolated hardware containers for sensitive credentials, which limits the damage that software-level compromise can cause. Studies from the International Telecommunication Union add that TPM integration improves device authentication and attestation in IoT architectures, but requires reliable supply chains and skilled maintenance to function effectively (ITU, 2024). These requirements become major constraints in low-resource environments.

Physically Unclonable Functions use microscopic manufacturing variations to generate device-unique responses. Gebali and Mamun (2022) describe PUFs as providing an intrinsic identity… impossible to replicate even by the original manufacturer. This makes them useful for authenticating large numbers of small, low-cost IoT devices. However, field studies also showed that PUF responses can

Citation: Adekunle, Adeogun A. ; Omori, Omini M. & Oluwaseun, Ayanniran F. "Hardware-Based Security Mechanisms for IoT Devices in Emerging Economies". *Journal of People and Worldviews (JPW),* 2026: pp115-126.

fluctuate with environmental factors. Shamsoshoara *et al.* (2020) reported that PUF values vary noticeably under changes in temperature and voltage, which requires additional error-correction layers for reliable use. These stability requirements pose challenges for regions where devices operate outdoors or under inconsistent environmental conditions.

IoT hardware designed for stable, well-resourced environments does not always perform well under the constraints common in developing regions. Laghari *et al.* (2024) observed that weak power infrastructure and inconsistent regulatory enforcement create vulnerabilities for IoT deployments in low-resource settings. Pourrahmani (2023) noted that hardware-embedded defenses frequently assume predictable manufacturing quality and secure provisioning processes that are not always guaranteed in emerging markets. Furthermore, Tondro *et al.* (2025) found that many IoT start-ups in developing economies struggle with technical capacity and supply-chain limitations that affect both device quality and the ability to maintain hardware-based security solutions.

These constraints reveal the structural challenges in implementing advanced hardware-rooted protections at scale in emerging economies. Across the literature, there is a clear gap in the empirical work examining how hardware-security mechanisms behave under real-world conditions in emerging economies. Much of the scholarship focuses on theoretical benefits or controlled laboratory evaluations. Lighter secure boot mechanisms are being developed for constrained environments, but their performance across variable power and environmental conditions remains understudied. Thus, there is a need for a more contextual understanding of how hardware-based IoT defenses can be adapted to suit infrastructure, economic realities, and skill availability in developing regions.

Theoretical Framework

The diffusion of innovation theory helps explain how new technologies spread across populations and why certain innovations gain traction while others face resistance. When applied to hardware-based IoT security, the theory emphasizes three important issues.

First, innovations that require specialized skills, higher costs, or complex infrastructure tend to diffuse slowly, especially in environments with limited resources. Second, adopters evaluate hardware security mechanisms based on their perceived compatibility with their existing systems and conditions. Therefore, early adopters influence broader uptake, which means that institutions or industries in emerging economies that lack early champions may experience slower adoption of secure hardware designs. This theory supports the argument that strong technical solutions alone do not guarantee adoption; perceived fit, cost and capacity shape whether hardware-rooted security becomes practical within emerging economies.

Socio-Technical Systems Theory, on the other hand, emphasizes the

interaction between human, organizational and technical components. This is relevant here because hardware-based security mechanisms do not operate in isolation. They rely on supporting human skills, organizational processes, regulatory structures, and supply chains. Applying this theory shows that IoT hardware security is influenced by social conditions such as technical expertise, maintenance culture, and institutional support. It also reveals that weaknesses in any part of the social or organizational environment can reduce the effectiveness of even the most robust hardware protections.

Hardware security rests on the assumption that devices can be trusted at their most fundamental layer. Trust models explain how systems establish and maintain confidence in devices, identities, and processes. Hardware-based mechanisms such as secure boot, device identity anchors and trusted execution environments create what is commonly referred to as a root of trust.

Risk management principles help clarify why such hardware anchors matter as they provide a baseline level of certainty that reduces the probability of catastrophic failures higher up the system. These principles also clarify why environments with weak infrastructure or unstable conditions face higher residual risks. Therefore, the trust and risk models support the study's focus by explaining both the potential reliability of hardware protections and the challenges that arise when they are deployed in resource-constrained environments.

Methodology

This study applied a systematic literature review design to examine the current state of hardware-based security mechanisms for IoT devices and to evaluate their suitability for emerging economies. The approach was guided by the theoretical framework, particularly the insights from Diffusion of Innovation Theory, Socio-Technical Systems Theory and Trust and Risk Models. These theories emphasize that the practical value of technological solutions depends not only on their technical properties but also on their contextual compatibility, which makes a systematic, structured review the most appropriate method for this investigation.

Research Design

A systematic literature review was selected because it provides a transparent and replicable process for gathering, evaluating, and synthesizing scholarly work. This design helps identify patterns, strengths, and gaps in existing knowledge while avoiding the selective bias that may arise from narrative or informal reviews. The nature of hardware-based IoT security, which spans multiple technical components, justified an approach that could organize and evaluate diverse findings coherently.

Search Strategy

The review process began with the development of a comprehensive set

of keywords and a search that captured both the technical and contextual elements of the topic. These terms included expressions relating to hardware security, device identity, secure boot, trusted execution environments, physically unclonable functions, cryptographic hardware, and IoT deployment challenges. The searches were conducted in reputable academic databases and digital libraries that specialize in engineering and technology research. To achieve relevance, the search focused on materials published within a defined timeframe and on sources that offered direct relevance to hardware-level IoT security.

Inclusion and Exclusion Criteria

Clear criteria guided which materials were selected for review. Studies were included if they examined hardware-based security techniques for the IoT, analyzed their effectiveness, or explored device-level trust mechanisms. Materials were excluded if they focused solely on software security, general networking issues, or unrelated cybersecurity topics. Priority was placed on peer-reviewed publications, technical evaluations, and studies that offered conceptual or practical insights relevant to hardware protection.

Screening and Evaluation Process

The screening involved reviewing titles and abstracts to determine their alignment with the topic. Full-text screening was followed to assess the methodological quality and thematic relevance. Each selected paper was then evaluated on the basis of its contribution to understanding hardware-rooted security, its discussion of practical constraints and the clarity of its findings. This systematic approach ensured that only credible and relevant studies informed the analysis.

Data extraction and synthesis

Key information was extracted from each study, including the hardware mechanism discussed, the problem it addressed, the deployment conditions and any identified limitations. The extracted data were then organized into thematic categories reflecting major security mechanisms, practical concerns and contextual constraints. Themes were synthesized to identify recurring patterns, strengths, weaknesses, and gaps in the existing work. Through this synthesis, the review connected technical findings with theoretical insights and the practical realities of emerging economies.

Findings

The review shows that hardware-rooted security mechanisms form the most reliable foundation for securing IoT devices, but adoption remains uneven and technically constrained. A central finding is that many IoT systems still lack dedicated hardware protection even though the security value of such mechanisms is well-demonstrated. A 2023 industry report confirms that 66% of all cellular IoT modules shipped worldwide in Q2 2023 contained no dedicated hardware security component, while 29% lacked any security features at all (IoT Analytics GmbH, 2023). This absence of basic hardware protections

means that a significant proportion of deployed IoT devices begin their lifecycle without hardware-anchored trust, leaving them susceptible to low-level exploits, unauthorized code loading, and identity spoofing.

Where hardware-based mechanisms are implemented, the literature shows that they provide strong, measurable improvements in device resilience. Secure boot techniques, for instance, consistently demonstrate effectiveness in preventing firmware manipulation. Ling *et al.* (2021) showed that secure boot and trusted boot architectures built on ARM TrustZone ensure that only authenticated firmware is executed and allow remote attestation of device integrity. The study stresses that these protections remain stable even in constrained processors as long as key provisioning and measurement values are maintained accurately. Similar technical strengths appear in work on trusted execution environments with Geppert *et al*. (2022) showing that TEEs provide isolated runtime environments that safeguard sensitive operations even when the operating system is compromised, strengthening confidentiality and integrity guarantees.

Lightweight authentication mechanisms based on the physical characteristics of the hardware also show practical potential. Shamsoshoara *et al*. (2020) demonstrated that physically unclonable functions can generate device-unique responses without storing long-term secrets, offering a low-cost way to authenticate constrained devices. However, they note that PUF reliability is sensitive to voltage, temperature and aging, requiring error-correction schemes to ensure stability over time. Gołofit (2024) extends this in a recent Scientific Reports article, showing that even "memoryless" IoT devices can implement PUF-based primitives and true random number generators to establish secure identities with minimal hardware overhead. These findings collectively suggest that PUFs represent one of the most feasible hardware security mechanisms for low-cost IoT deployments.

The review also identifies the operational and environmental constraints that limit the consistent performance of the hardware-based mechanisms. Pourrahmani and Yavarinasab (2023) observed that many IoT systems assume conditions such as stable power supply, reliable update channels and predictable environmental behavior assumptions that do not always hold in diverse deployment contexts. The point is that hardware-rooted protections, while robust in design, depend on secure provisioning, manufacturing quality and maintenance processes that must remain reliable across the device lifecycle. When these supporting conditions break down, even strong hardware primitives underperform or become challenging to manage.

The findings demonstrate that hardware-rooted IoT security mechanisms such as secure boot, trusted execution environments, PUFs and hardware-based identity modules are technically sound and effective. However, their adoption at scale is limited by cost, supply-chain

dependencies, environmental sensitivities, and infrastructural requirements. The evidence points to a widening gap between the technical strength of available hardware-security features and the prevalence of real-world deployments that lack them. This underscores the need for adaptable, context-aware hardware-security strategies for settings where resources and conditions vary significantly.

Discussion

The findings point to a consistent pattern that hardware-based IoT security mechanisms are technically reliable, with their adoption and real-world performance depending on structural and environmental factors that vary widely across contexts. The industry report showing that most IoT modules still ship without hardware security (IoT Analytics GmbH, 2023) points to the systemic lag between available technology and deployment trends. This adoption gap reflects not only production costs but also the uncertainty among manufacturers about integrating hardware trust anchors into low-cost devices.

A central insight from the findings is that a secure boot, trusted execution environments and physically unclonable functions deliver demonstrable gains in device integrity. Studies such as those by Ling *et al.* (2021) and Geppert *et al.* (2022) confirm that hardware isolation layers can maintain trustworthy execution states even when other software layers fail. These technologies succeed because they create security guarantees independent of the main operating system. As the theoretical framework suggests, innovations requiring new manufacturing processes, firmware signing infrastructure, or specialized skill sets will diffuse more slowly in environments where capacity is uneven.

The findings also show that the operational conditions in which IoT devices function play a critical role in the effectiveness of these protections. As noted earlier, PUF-based authentication can be sensitive to environmental factors, and this concern is strengthened by broader security analyses. The European Union Agency for Cybersecurity observes in its ENISA Threat Landscape for IoT (2022) that environmental instability and inconsistent component quality remain major contributors to IoT hardware vulnerabilities across global markets. This aligns with the empirical findings of Shamsoshoara *et al.* (2020) and Gołofit (2024), who showed that PUF reliability depends on controlled operating conditions.

Furthermore, the structural challenges identified in the findings are echoed in the international cybersecurity guidance. The NISTIR 8259 series (NIST, 2020) emphasizes that secure hardware capabilities require lifecycle support provisioning, update mechanisms, and continuous monitoring. These requirements are not easily met in settings with limited infrastructure or where devices operate in remote areas without consistent maintenance. The difficulty of providing reliable firmware updates, for example, means that secure boot chains may degrade over time if measurement values cannot be refreshed or authenticated reliably.

Citation: Adekunle, Adeogun A. ; Omori, Omini M. & Oluwaseun, Ayanniran F. "Hardware-Based Security Mechanisms for IoT Devices in Emerging Economies". *Journal of People and Worldviews (JPW),* 2026: pp115-126.

Complementing this, the GSMA IoT Security Guidelines (GSMA, 2021) note that cost pressures in the IoT market lead many manufacturers to avoid implementing secure elements, trusted execution support, or hardware-backed identities. This industry perspective explains why even technically strong mechanisms fail to appear widely in deployed devices. The motivations extend beyond technical capability into market incentives and manufacturing economics.

These sources support the argument that hardware-based IoT security, though mature and effective, cannot be separated from the socio-technical systems in which devices operate. The theoretical expectation that innovation adoption depends on compatibility, cost, and support structures is reflected in real-world deployment patterns. The hardware protections examined in the findings offer credible trust anchors, even though their practical value is shaped by environmental conditions, supply-chain decisions and institutional capacity. This explains why strong mechanisms coexist with widespread under implementation and underscores the need for adaptive hardware security frameworks that account for the constraints of emerging and resource-variable environments.

Conclusion

This study aimed to understand how hardware-based security mechanisms protect IoT devices and how these mechanisms perform under the conditions typical of emerging economies. The review and analysis demonstrate that hardware-rooted protections such as secure boot, trusted execution environments and physically unclonable functions provide a strong foundation for device trust by anchoring identity, integrity and key material in silicon rather than software alone. These mechanisms close entire classes of attacks that exploit low-level compromise, unauthorized firmware modification, or device impersonation, confirming their centrality to modern IoT security.

However, the findings also show that the presence of capable technologies does not automatically translate into widespread or effective deployment. A significant proportion of IoT modules still ship without any dedicated hardware security, explaining why many devices begin their operational life with structural vulnerabilities. The technical literature makes clear that even the most robust hardware primitives depend on stable provisioning, reliable update mechanisms, predictable environmental conditions, and a supporting ecosystem of skills and processes. Where these conditions are weak, the practical value of hardware security diminishes, and devices struggle to maintain the trust models they were designed around.

The theoretical framework helps clarify this gap with the diffusion of innovation theory explaining why cost, compatibility and perceived complexity slow adoption, especially in markets where manufacturers prioritize affordability. Socio-technical systems theory also shows that hardware

Citation: Adekunle, Adeogun A. ; Omori, Omini M. & Oluwaseun, Ayanniran F. "Hardware-Based Security Mechanisms for IoT Devices in Emerging Economies". *Journal of People and Worldviews (JPW),* 2026: pp115-126.

security must interact with organizational processes, maintenance culture and environmental realities, which vary widely across deployment regions. Risk and trust models reveal that the hardware roots of trust can only sustain their guarantees when the broader lifecycle and operating conditions remain reliable. The study therefore takes the direction that strengthening hardware security in IoT systems for emerging economies demands a blend of technical excellence and contextual awareness. Where hardware-based protections are adapted thoughtfully and supported by appropriate processes, they offer a path toward durable, scalable, and trustworthy IoT environments capable of supporting development goals and digital transformation efforts in diverse environments.

Recommendations

The analysis shows that hardware-based security mechanisms are technically sound but are unevenly adopted and sensitive to deployment conditions. Therefore, strengthening IoT security in emerging economies requires measures that address both the hardware itself and the systems surrounding it. The following recommendations become germane to informing practice:

i. Promote low-cost, scalable hardware security designs

Manufacturers serving emerging markets should prioritize implementing lightweight hardware primitives that offer strong protection without significant cost increases. Mechanisms such as physically unclonable functions, small secure elements, and simplified secure boot chains can be integrated into low-cost devices without major redesigns.

ii. Strengthen the local supply chain and provisioning capacity

Hardware-rooted security depends on secure provisioning, reliable update pathways, and consistent device quality. Countries and regional markets should work toward developing local or regional provisioning services, certification bodies, and integration hubs that ensure device keys are generated, stored, and managed securely. This reduces dependence on foreign supply chains and mitigates the risks associated with inconsistent manufacturing practices.

iii. Build technical capacity for hardware security management

Emerging economies require targeted investment in skills development to manage secure hardware mechanisms throughout device lifecycles. Training programs for technicians, engineers, and system administrators can focus on secure firmware signing, update validation, attestation verification, and environmental diagnostics. When technical personnel understand the hardware trust anchors and lifecycle requirements, the devices are more likely to remain secure after deployment.

iv. Encourage public–private partnerships to reduce the implementation cost

Citation: Adekunle, Adeogun A. ; Omori, Omini M. & Oluwaseun, Ayanniran F. "Hardware-Based Security Mechanisms for IoT Devices in Emerging Economies". *Journal of People and Worldviews (JPW),* 2026: pp115-126.

Given the financial constraints common in emerging economies, shared investment models can help distribute the cost of integrating hardware security. Governments, private-sector partners, telecom operators, and IoT solution providers can collaborate on secure provisioning centers, firmware update infrastructure, and trust systems. These collaborative structures can reduce the cost burden of individual manufacturers and speed up the diffusion of secure hardware technologies.

References

Chatterjee, D. (2025). Hardware Security in the Connected World. *WIRE Security and Privacy*, Article 70034.

Gebali, F., & Mamun, M. (2022). Review of Physically Unclonable Functions: Structures, models, and algorithms *Frontiers in Sensors*, 3, 751748.

Geppert, T., Deml, S., Sturzenegger, D., & Ebert, N. (2022). Trusted execution environments: Applications and organizational challenges. *Frontiers in Computer Science*, 4, Article 930741. https://doi.org/10.3389/fcomp.2022.930741

Gołofit, K. (2024). Security primitives for memoryless IoT devices based on physical unclonable functions and true random number generators. *Scientific Reports*, 14, Article 24060. doi:10.1038/s41598-024-75373-6

GSMA. (2021). GSMA IoT Security Guidelines. GSM Association.

International Telecommunication Union (ITU). (2024). Optimizing IoT security via TPM integration. *ITU Journal*, 5(1), 1–14.

IoT Analytics GmbH. (2023). Cellular IoT module market Q2 2023: 66% of modules shipped without dedicated hardware security. Hamburg, Germany.

Laghari, A. A., et al. (2024). Internet of Things (IoT) applications security trends and challenges. *Discover the Internet of Things*, 4, Article 36.

Ling, Z., et al. (2021). Secure boot, trusted boot, and remote attestation for the ARM TrustZone. *Journal of Systems Architecture*, 119, 101271.

NIST. (2020). NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers. National Institute of Standards and Technology.

Pourrahmani, H., & Yavarinasab, A. (2023). A review of the security vulnerabilities and countermeasures in the Internet of Things solutions. *Internet of Things*, 23, 100888. doi:10.1016/j.iot.2023.100888

Shamsoshoara, A., Korenda, A., Afghah, F., & Zeadally, S. (2020). A survey on physical unclonable function (PUF)-based security solutions for the Internet of Things *Computer Networks*, 183, 107593. doi:10.1016/j.comnet.2020.107593

Tondro, M., Jahanbakht, M., & Ozay, D. (2025). Enhancing IoT Technology Acquisition in Emerging Economies: Insights and Recommendations Using an Analytical Case Study Review of IoT Startups *Businesses*, 5(2), 20.

Williams, P. (2022). A survey on security in the internet of things with a focus on hardware aspects. *Electronics (Switzerland)*, 11(159), Article 159.

Citation: Adekunle, Adeogun A. ; Omori, Omini M. & Oluwaseun, Ayanniran F. "Hardware-Based Security Mechanisms for IoT Devices in Emerging Economies". *Journal of People and Worldviews (JPW),* 2026: pp115-126.