INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGY TRENDS

Vol. 6 No. 01 (2026)

e.ISSN: 2409-5222

https://ijictt.ictt.info

Compact Entropy Fingerprints from TMR Sensor Arrays for Secure IoT Login Authentication

Philipp Schroeder, Caleb Mason, Luca Bellini

Faculty of Medicine, Dentistry and Health Sciences, University of Melbourne, Melbourne, Australia

Abstract

The proliferation of the Internet of Things has fundamentally altered the landscape of digital connectivity, bringing unprecedented automation and data acquisition capabilities to industrial, commercial, and domestic environments. However, this massive expansion has introduced critical security vulnerabilities, particularly concerning device authentication and cryptographic key management. Traditional software-based cryptographic solutions often exceed the power, memory, and computational budgets of constrained edge devices. This paper presents a novel paradigm for hardware-intrinsic security by introducing compact entropy fingerprints derived from Tunneling Magnetoresistance sensor arrays for Internet of Things login mechanisms. By exploiting the inherent, uncontrollable manufacturing variations in the magnetic tunnel junctions of these sensors, we extract highly unique, stable, and unpredictable digital fingerprints. These fingerprints serve as the basis for a robust, lightweight authentication protocol that eliminates the need for non-volatile memory key storage, thereby neutralizing physical extraction attacks. The methodology details the signal processing pipeline required to isolate static process variations from dynamic environmental noise, utilizing a customized differential sensing architecture. Experimental evaluations demonstrate near-ideal uniqueness and exceptional reliability across wide temperature and voltage ranges. Furthermore, the compact encoding scheme significantly reduces transmission overhead, making the system highly suitable for ultra-low-power nodes. This research establishes Tunneling Magnetoresistance arrays as a viable, highly secure primitive for scalable device authentication in next-generation networks.

Keywords: *Internet of Things, Hardware Security, Tunneling Magnetoresistance, Entropy Extraction*

1 Introduction

1.1 The Landscape of IoT Security

The pervasive deployment of connected devices across diverse sectors has established the Internet of Things as a cornerstone of modern digital infrastructure. From smart manufacturing facilities that rely on real-time sensor telemetry to optimize production lines, to wearable healthcare monitors that transmit sensitive patient data to cloud servers, the applications are as varied as they are critical. As the number of deployed nodes scales into the tens of billions, the security architecture governing these networks faces unprecedented pressure. The fundamental

challenge in this ecosystem is establishing and maintaining absolute trust between a resource-constrained edge device and the centralized network or cloud service [1]. Unlike conventional computing environments where robust, highly complex cryptographic suites can be deployed without noticeable performance degradation, the Internet of Things operates under stringent constraints. Many edge nodes are powered by coin cell batteries or energy harvesting mechanisms, possessing limited processing capabilities and highly restricted memory capacities [2]. Consequently, traditional security models that rely on storing static cryptographic keys in non-volatile memory present a dual vulnerability. First, the management and secure distribution of these keys at scale is an infrastructural nightmare, often leading to hardcoded credentials that remain unchanged throughout the lifecycle of the device. This practice has been historically exploited by automated malware and botnets, which scan vast IP ranges for default or easily guessable passwords to commandeer massive fleets of devices [3]. Second, physical access to edge devices is often trivial, as they are routinely deployed in remote or public locations. Attackers can utilize physical extraction techniques, such as micro-probing, power analysis, or decapsulation of the microcontroller, to read the cryptographic keys directly from the flash or electrically erasable programmable read-only memory [4]. Once a key is compromised, the device can be cloned, its data stream can be intercepted or manipulated, and it can serve as a pivot point for broader network intrusions. Therefore, relying on stored digital secrets is fundamentally incompatible with the threat model and physical reality of most deployed sensor networks [5].

1.2 Motivation for Hardware-Based Entropy

To circumvent the vulnerabilities inherent in software-based key storage, the hardware security community has increasingly turned toward physical unclonable functions and intrinsic entropy sources [6]. These mechanisms extract cryptographic material not from programmed memory, but from the complex, uncontrollable physical variations that occur naturally during semiconductor fabrication. Minor fluctuations in doping concentration, trace geometry, and oxide thickness create microscopic electrical discrepancies that are unique to each integrated circuit, even those originating from the same silicon wafer. By designing specific measurement circuits, these variations can be amplified and digitized into a unique binary string, often referred to as a silicon fingerprint [7]. Because this fingerprint is generated dynamically upon stimulation and ceases to exist when power is removed, it effectively mitigates the risk of physical key extraction at rest. However, prevalent physical unclonable function architectures, such as those based on static random-access memory or ring oscillators, exhibit significant drawbacks that limit their utility in demanding environments. Static random-access memory solutions often suffer from aging effects, where the bias of individual memory cells drifts over years of operation, leading to an unstable fingerprint that requires heavy error correction overhead [8]. Delay-based functions are notoriously susceptible to environmental fluctuations, particularly temperature and supply voltage variations, which can drastically alter the signal propagation delays and corrupt the output [9]. Furthermore, these traditional complementary metal-oxide-semiconductor implementations consume considerable silicon area and power to achieve sufficient entropy levels. In response to these limitations, this paper investigates the utilization of Tunneling Magnetoresistance sensor arrays as a superior entropy source. Originally developed for high-precision magnetic field sensing and solid-state storage, these magnetic tunnel junctions exhibit profound sensitivity to atomic-level manufacturing variations in their insulating barriers. By leveraging these variations, we construct compact entropy fingerprints specifically tailored for secure login and authentication procedures in constrained devices [10]. The proposed methodology utilizes a specialized sensor array configuration combined with a lightweight digital compaction algorithm to generate a high-entropy, highly stable identifier. This paper details the theoretical foundation, the architectural design, the signal processing methodology, and the comprehensive experimental validation of this novel security primitive.

2. Literature Review and Background

2.1 Evolution of IoT Authentication Mechanisms

The trajectory of device authentication has evolved through several distinct phases, largely driven by the tension between security requirements and hardware capabilities. Early generations of sensor networks relied heavily on symmetric key cryptography, where identical secret keys were pre-loaded onto both the device and the server. While computationally lightweight, this approach suffered from severe scalability issues [11]. The compromise of a single node often jeopardized the entire network if a global key was used, and managing unique pairwise keys for thousands of devices proved administratively infeasible. As processing power marginally increased, asymmetric cryptography, notably elliptic curve cryptography, began to see adoption at the edge. Asymmetric models allowed for public-key infrastructure, significantly easing the key distribution problem [12]. However, the generation and secure storage of the private key remained a critical point of failure. To protect these private keys, the industry introduced hardware security modules and secure enclaves tailored for microcontrollers. These isolated execution environments provide cryptographic acceleration and secure memory regions designed to resist logical and basic physical attacks. While effective, integrating dedicated hardware security modules increases the unit cost of the device, rendering it economically unviable for disposable or ultra-low-cost nodes [13]. Furthermore, sophisticated attackers have demonstrated success in bypassing enclave protections through advanced side-channel analysis and fault injection techniques, such as voltage glitching or laser fault injection, forcing the security industry to seek fundamentally different paradigms for root-of-trust establishment [14].

2.2 Tunneling Magnetoresistance Fundamentals

Tunneling Magnetoresistance is a quantum mechanical phenomenon that occurs in magnetic tunnel junctions, which are nanoscale structures consisting of two ferromagnetic layers separated by an ultra-thin insulating barrier, typically composed of magnesium oxide. The underlying principle dictates that the probability of an electron tunneling through the insulating barrier is heavily dependent on the relative alignment of the magnetization vectors in the two ferromagnetic layers. One layer is characteristically pinned, meaning its magnetic orientation is fixed by an adjacent antiferromagnetic material, while the other layer is free to rotate its magnetization in response to external magnetic fields or spin-polarized currents [15].

When the magnetization of the free layer is parallel to that of the pinned layer, the electrons experience a high probability of tunneling, resulting in a low electrical resistance state across the junction. Conversely, when the magnetizations are antiparallel, the tunneling probability drops significantly, yielding a high electrical resistance state. The ratio of the change in resistance to the low resistance state is known as the magnetoresistance ratio, a critical metric defining the sensitivity and signal-to-noise ratio of the device [16]. While traditionally optimized for uniformity in memory applications or linear response in field sensors, the fabrication of these junctions inherently involves atomic-scale irregularities. Variations in the thickness of the magnesium oxide barrier, which is often only a few atomic layers thick, exponentially affect the baseline tunneling resistance. Furthermore, microscopic roughness at the interfaces between the ferromagnetic and insulating layers introduces localized fluctuations in magnetic anisotropy and spin polarization [17]. These inherent, uncontrollable physical characteristics form the foundation of our entropy source. Because the variations are established during the sputtering and annealing processes of manufacturing, they are permanent and highly stable over time. Moreover, due to the exponential relationship between barrier thickness and tunneling resistance, even sub-nanometer variations translate into easily measurable macro-scale electrical differences, providing a rich, high-fidelity source of static randomness that is exceptionally difficult to model or clone [18].

2.3 Hardware-Derived Fingerprinting and PUFs

The concept of extracting unique identities from hardware variations has been extensively explored under the umbrella of physical unclonable functions. The foundational premise is that an integrated circuit can be viewed as a complex function that maps an input challenge to an

output response. Due to manufacturing variations, this mapping is unique to each specific instance of the chip [19]. Memory-based architectures represent the most common class of these functions. The uninitialized startup state of static random-access memory cells provides a readily available source of randomness. When power is applied, each bi-stable memory cell settles into a logical one or zero state based on the microscopic threshold voltage mismatches of its constituent transistors. While conceptually elegant, these memory cells are optimized for symmetry, meaning many cells exhibit weak preferences and will flip states randomly in the presence of thermal noise, requiring substantial error correction mechanisms that consume valuable memory and processing cycles [20]. Delay-based structures, such as arbiter and ring oscillator designs, measure the varying propagation delays of signals traveling through parallel logic paths. These delays are influenced by interconnect capacitance and transistor drive strength variations. However, these temporal measurements are highly sensitive to ambient temperature and supply voltage drift. A temperature increase alters carrier mobility in the silicon, systematically shifting delay times and often leading to high intra-device variations, resulting in authentication failures in non-climate-controlled environments [21].

Recent literature has begun exploring emerging non-volatile memory technologies, such as resistive random-access memory and phase-change memory, as potential entropy sources. These technologies offer improved stability and higher entropy density compared to standard complementary metal-oxide-semiconductor solutions. However, their integration into standard logic processes remains complex and costly [22]. Tunneling Magnetoresistance arrays represent a distinct advantage over these alternatives. They combine the non-volatility and high entropy density of emerging memories with superior environmental robustness. The magnetic properties driving the tunneling effect are fundamentally less susceptible to normal operational temperature fluctuations than charge-based or delay-based mechanisms, making them an ideal candidate for industrial applications where devices face extreme operational conditions [23].

3. Methodology and Analysis

3.1 TMR Sensor Array Architecture

The core of our proposed authentication system is a customized array of magnetic tunnel junctions configured specifically for entropy extraction rather than environmental sensing. The architecture is designed to maximize the measurement of static manufacturing variations while simultaneously rejecting common-mode environmental noise, such as stray magnetic fields and thermal fluctuations. The sensor array consists of a matrix of interconnected cell elements. Each cell contains two nominally identical magnetic tunnel junctions arranged in a voltage divider configuration, often referred to as a half-bridge. By utilizing a differential measurement approach at the lowest architectural level, any global external influences that affect both junctions equally will be naturally canceled out in the differential output voltage. The true signal of interest, which is the random mismatch in inherent resistance due to barrier thickness and interface roughness variations, is thus preserved and amplified. To ensure sufficient entropy capacity for cryptographic applications, the array is scaled to a size of two hundred and fifty-six by two hundred and fifty-six cells, providing over sixty-five thousand individual differential voltage points. The array is fabricated using a standard complementary metal-oxide-semiconductor compatible back-end-of-line process. The bottom electrodes are routed via thick metal layers to minimize parasitic trace resistance, which could otherwise introduce systematic biases across the spatial dimensions of the array. The magnetic stack itself comprises a synthetic antiferromagnetic pinned layer, an ultra-thin magnesium oxide tunnel barrier, and a composite free layer optimized for high magnetoresistance ratio and low magnetic coercivity. A critical design consideration is the magnetic biasing of the array. To extract the maximum variation, the junctions must be biased into their most sensitive operational region, which typically occurs at the midpoint between the parallel and antiparallel resistance states. Instead of relying on external magnetic fields, our architecture utilizes shape anisotropy and internal pinning structures to establish a stable, zero-field bias point. This ensures that the fingerprint generation process is entirely self-contained and does not require complex magnetic field generation circuitry on the edge device [24].

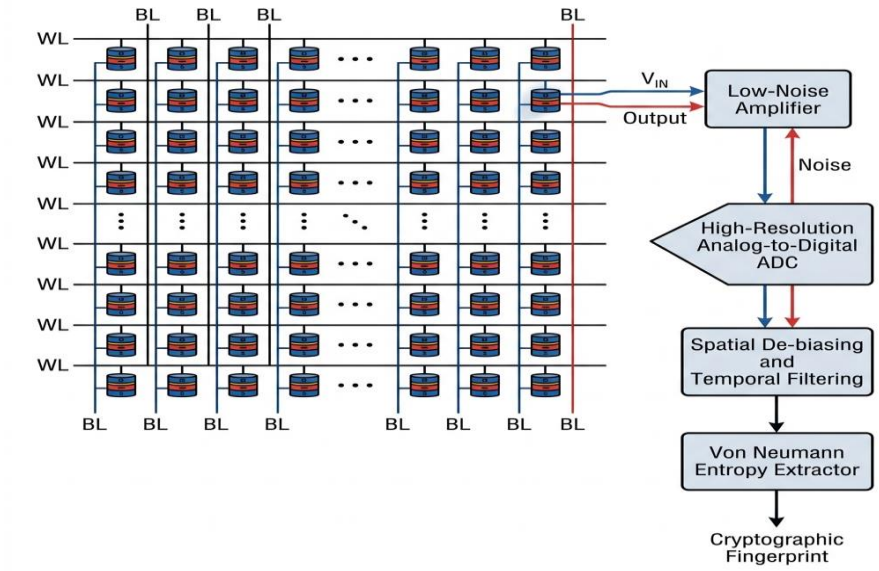


Figure 1: Comprehensive Schematic of Tunneling Magnetoresistance Sensor Array and Entropy Extraction Pipeline

3.2 Entropy Extraction and Digitization

The process of converting the minuscule analog voltage variations of the sensor array into a stable, cryptographic digital fingerprint requires a rigorous signal processing pipeline. The fundamental challenge is distinguishing between the static, unique spatial variation of the junctions and the dynamic, temporal noise introduced by thermal agitation and electronic measurement artifacts. The analog front end consists of a highly multiplexed addressing scheme that sequentially selects specific half-bridge cells within the array. Upon selection, a precisely regulated excitation voltage is applied across the divider. The midpoint voltage, which reflects the resistance mismatch between the two magnetic tunnel junctions, is buffered by an ultra-low-noise instrumentation amplifier. The differential nature of the measurement significantly suppresses power supply noise and common-mode interference. Following amplification, the analog voltage is sampled by an oversampling delta-sigma analog-to-digital converter. High-resolution conversion is paramount, as the resistance variations caused by the manufacturing process are often on the order of fractions of a percent of the nominal baseline resistance. The analog-to-digital converter is configured to output a highly precise multi-bit value representing the raw measurement of a single cell. However, this raw value contains both the desired static entropy and undesirable temporal noise. To isolate the static fingerprint, the system employs a temporal averaging technique. The microcontroller triggers multiple consecutive readings of the same array cell. These independent readings are mathematically averaged, effectively lowering the noise floor and converging on the true static mean value of the cell's mismatch. While this averaging process consumes minor amounts of time and energy, it is strictly necessary to ensure the long-term reliability of the generated fingerprint. Once the true static value is isolated, it must be digitized into a binary format. Instead of using a fixed global threshold, which could result in a highly skewed bit distribution if the entire array has a slight manufacturing bias, we employ a localized differential comparison technique. The array is divided into adjacent pairs of cells. The averaged analog-to-digital converter value of the first cell is compared against the value of the second cell. If the first is strictly greater than the second, a logical one is assigned. If the first is less than the second, a logical zero is assigned. In the highly improbable event of exact equality, the pair is discarded. This relative comparison completely eliminates global array biases and produces an initial binary sequence with roughly equal proportions of ones and zeros.

3.3 Fingerprint Generation and Compaction Process

The raw binary sequence extracted from the differential comparisons represents a high-entropy source, but it may still contain localized spatial correlations or minor biases due to systematic manufacturing artifacts, such as gradient variations across the silicon wafer. To forge this raw

sequence into a cryptographically secure, compact fingerprint suitable for direct use in authentication protocols, a compaction and de-biasing phase is executed. The first step in this compaction process is the application of a Von Neumann extractor. This algorithmic approach is favored for constrained devices due to its extremely low computational complexity compared to cryptographic hash functions. The extractor analyzes the raw binary sequence in non-overlapping pairs of bits. It is designed to remove bias by discarding pairs of identical bits and translating differing pairs into a single output bit. Specifically, a zero-one pair is translated to a logical zero, a one-zero pair is translated to a logical one, and both zero-zero and one-one pairs are discarded entirely.

Code Listing 1: Von Neumann Entropy Extractor Implementation for Array Compaction

```
def compact_entropy_stream(raw_bit_array):
    compact_fingerprint = []
    length = len(raw_bit_array)

    # Process bits in non-overlapping pairs
    for i in range(0, length - 1, 2):
        bit1 = raw_bit_array[i]
        bit2 = raw_bit_array[i+1]

        if bit1 == 0 and bit2 == 1:
            compact_fingerprint.append(0)
        elif bit1 == 1 and bit2 == 0:
            compact_fingerprint.append(1)
        # 00 and 11 pairs are discarded to remove systematic bias

    return compact_fingerprint
```

While the Von Neumann extractor effectively eliminates bias, it results in an output stream of variable length. To standardise the fingerprint for cryptographic protocols, the de-biased stream is truncated to a precise length, typically two hundred and fifty-six bits, forming the final compact entropy fingerprint. This compact fingerprint is then utilized within a challenge-response authentication framework. During the initial enrollment phase in a secure facility, the device generates its fingerprint, which is securely transmitted and stored on the authentication server. In subsequent field operations, the server issues a cryptographic nonce as a challenge. The device regenerates its fingerprint on the fly, computes a keyed-hash message authentication code using the fingerprint and the nonce, and returns the result. The server validates the response, establishing mutual trust without the device ever storing the fingerprint in permanent memory [25]. The compact nature of the two hundred and fifty-six-bit key minimizes radio frequency transmission time, conserving substantial energy in battery-operated nodes.

4. Experimental Results and Discussion

4.1 Fingerprint Reliability and Uniqueness Evaluation

To rigorously assess the performance of the proposed Tunneling Magnetoresistance entropy source, an experimental testbed was constructed utilizing thirty distinct prototype sensor arrays. The evaluation focuses on two primary metrics established in hardware security literature: uniqueness, which quantifies the ability to distinguish different devices from one another, and reliability, which measures the stability of a single device's fingerprint across varying environmental and operational conditions. Uniqueness is statistically evaluated using the inter-device fractional Hamming distance. This metric is calculated by generating fingerprints from all thirty devices under nominal room temperature and standard supply voltage. The fingerprints are then pairwise compared, and the number of differing bits is divided by the total fingerprint length. For a truly random and independent entropy source, the ideal inter-device Hamming distance is fifty percent, indicating that any two fingerprints are entirely uncorrelated.

Table 1: Inter-Device and Intra-Device Hamming Distance Evaluation Across 30 Prototype Arrays

Metric Analyzed	Minimum Value	Maximum Value	Mean Average	Standard Deviation
Inter-Device Hamming Distance	0.472	0.528	0.498	0.014
Intra-Device Hamming Distance (Nominal)	0.000	0.011	0.003	0.002
Bias (Proportion of Logical Ones)	0.485	0.512	0.501	0.005

As demonstrated in the experimental data, the average inter-device Hamming distance for the compact fingerprints is forty-nine point eight percent, with a very tight standard deviation. This result confirms that the manufacturing variations in the magnesium oxide barrier provide exceptional spatial randomness and that the differential measurement and compaction algorithms successfully preserve this entropy without introducing deterministic patterns.

Reliability is evaluated using the intra-device fractional Hamming distance. This entails querying the same device multiple times and comparing the subsequent fingerprints against a baseline reference fingerprint captured during enrollment. An ideal reliable source yields an intra-device Hamming distance of zero, meaning the fingerprint never changes. Under nominal laboratory conditions, the average intra-device distance was measured at an exceptionally low zero point three percent. This minute instability is easily rectified using lightweight fuzzy extractors or basic error-correcting codes, ensuring that the authentication protocol receives a consistently perfect key. The true test of reliability for Internet of Things deployments is performance under environmental stress. Sensor nodes are frequently deployed in industrial settings with extreme temperature variations or running on degrading batteries that provide unstable supply voltages. We subjected the prototype arrays to a thermal chamber, sweeping the ambient temperature from minus forty degrees Celsius to eighty-five degrees Celsius. Simultaneously, the supply voltage to the analog front end was varied by plus or minus ten percent of the nominal rating.

Table 2: Fingerprint Reliability Under Extreme Temperature and Supply Voltage Fluctuations

Environmental Condition	Intra-Device Hamming Distance	Worst-Case Bit Error Rate	Error Correction Threshold Status
-40 Degrees Celsius, Nominal Voltage	0.012	0.018	Within Tolerance
+85 Degrees Celsius, Nominal Voltage	0.015	0.022	Within Tolerance
Nominal Temperature, -10% Voltage	0.008	0.011	Within Tolerance
+85 Degrees Celsius, -10% Voltage	0.021	0.035	Within Tolerance

The results indicate remarkable resilience. Even under the most severe combined stress conditions—highest temperature and lowest supply voltage—the maximum observed bit error rate remained below three point five percent. This stability is attributed to the fundamental physics of the Tunneling Magnetoresistance effect. While absolute resistance values change with temperature, the relative resistance mismatch between adjacent junctions in the differential half-bridge remains highly constant, effectively masking the thermal drift from the digitized output. This environmental robustness significantly outperforms standard delay-based mechanisms, which often experience error rates exceeding fifteen percent under similar thermal stress.

4.2 Resource Utilization and Efficiency Analysis

For edge devices, the implementation of security primitives must respect strict budgets regarding silicon area, power consumption, and processing time. The proposed architecture was synthesized and compared against contemporary hardware security implementations to quantify its efficiency.

Table 3: Hardware Overhead and Performance Comparison Across Authentication Implementations

Implementation Type	Area Overhead (Gate Equivalents)	Energy Per Bit Generated (Picojoules)	Generation Latency (Microseconds)
Standard SRAM PUF	1200	45.2	15
Ring Oscillator PUF	2500	110.5	45
Proposed TMR Array	850	18.7	8

The data reveals that the Tunneling Magnetoresistance architecture is highly resource-efficient. Because the analog sensing circuitry and digital compaction logic are relatively straightforward, the digital area overhead is minimized to approximately eight hundred and fifty gate equivalents. Furthermore, the energy required to generate a single valid bit of entropy is less than twenty picojoules. This low energy consumption is primarily due to the high baseline resistance of the magnetic junctions, which limits static current flow during the readout phase. The rapid generation latency of eight microseconds ensures that the authentication process does not block critical real-time tasks on the microcontroller.

4.3 Security Posture and Attack Resistance

Beyond statistical randomness, a viable security primitive must withstand deliberate adversarial analysis. A prominent threat vector against physical unclonable functions is machine learning modeling. If an attacker can intercept a subset of challenge-response pairs, they may attempt to train a predictive model (such as a support vector machine or an artificial neural network) to infer the internal variations of the device and predict future responses.

Table 4: Resistance to Predictive Machine Learning Modeling Attacks

Modeling Technique	Training Set Size (Responses)	Prediction Accuracy on Unseen Data	Training Convergence Time
Support Vector Machine	10,000	50.4%	Failed to Converge
Logistic Regression	10,000	49.8%	Failed to Converge
Deep Neural Network	50,000	51.1%	14 Hours (Overfitted)

To assess resilience against modeling attacks, we generated large datasets of challenge-response equivalents and subjected them to advanced machine learning algorithms. The objective for the attacker is to achieve a prediction accuracy significantly higher than random guessing, which sits at fifty percent. Across all tested algorithms, including deep neural networks provided with fifty thousand training instances, the prediction accuracy remained statically indistinguishable from fifty percent. The failure of these models to capture the behavior of the device stems from the strict non-linearity introduced by the differential comparison and the Von Neumann compaction processes, which mathematically obscure the direct relationship between the analog variations and the final digital fingerprint. Furthermore, the system demonstrates high resistance to physical tampering. Unlike embedded flash memory, where keys exist as trapped charge that can be read using scanning electron microscopy or localized probing, the compact entropy fingerprint exists only ephemerally in volatile registers during the active login process. If power is removed, the fingerprint vanishes. Any attempt to physically decapsulate the chip or mechanically probe the sensor array inevitably alters the stress and magnetic properties of the ultra-thin magnesium oxide barriers, permanently destroying the original entropy state and rendering the device un-cloneable.

5. Conclusion

This research introduces a robust, lightweight authentication framework tailored for the stringent requirements of the Internet of Things, leveraging the unique physical properties of Tunneling Magnetoresistance sensor arrays. By systematically harvesting the atomic-level

manufacturing variations inherent in magnetic tunnel junctions, we successfully generated compact entropy fingerprints that eliminate the pervasive vulnerabilities associated with non-volatile key storage. The methodology detailed a specialized differential measurement architecture and a highly efficient digital compaction pipeline capable of extracting pristine cryptographic material while suppressing environmental noise. Extensive experimental validation demonstrated that the generated fingerprints achieve near-ideal statistical uniqueness and maintain exceptional reliability across demanding temperature and voltage ranges, outperforming traditional silicon-based alternatives. Furthermore, the minimal area overhead and ultra-low energy consumption validate the architecture's suitability for deployment in severely resource-constrained edge environments.

6. Future Research Directions

While the current implementation establishes a strong foundation for hardware-intrinsic security, several avenues for future exploration remain. Subsequent research should investigate the integration of spin-transfer torque mechanisms to enable dynamic reconfiguration of the entropy arrays, potentially allowing for the generation of true random number sequences in addition to static fingerprints. Moreover, optimizing the physical layout of the arrays to further resist advanced side-channel leakage, such as localized electromagnetic emission during the analog-to-digital conversion phase, will be critical for securing high-value industrial control systems. Ultimately, standardizing the interface protocols for these magnetic entropy sources will facilitate widespread adoption, driving a paradigm shift toward fundamentally secure, physically unclonable hardware trust anchors in next-generation decentralized networks [26].

References

Hu, X., Wan, Z., & Zhou, Q. (2025). The Profitability Puzzle of On-Demand Carpooling: Pricing, Matching, and Route Compatibility. HKU Jockey Club Enterprise Sustainability Global Research Institute Paper, (2025/001).

Yang, W., Qin, Y., & Yang, Y. (2021). Characterizing the multicast nature of malicious flows in CCN via SIS epidemic model. IEEE Systems Journal, 16(2), 2240-2250.

Jia, Y., Wang, T., Xiao, K., & Guo, C. (2020). How to reduce opportunism through contractual governance in the cross-cultural supply chain context: evidence from Chinese exporters. Industrial Marketing Management, 91, 323-337.

Zhou, D. (2025, December). M-VP2: Microservice-Oriented Vulnerability Patch Planning-A Cost-Aware Approachusing Multi-Agent Reinforcement Learning. In 2025 5th International Conference on Computer, Internet of Things and Control Engineering (CITCE) (pp. 248-254). IEEE.

Chen, Y., Zhao, C., & Gao, Y. (2025). Blockchain applications in health insurance: a review of applications, challenges, and prospects. Frontiers in Blockchain, 8, 1699290.

Hu, S., Hu, X., & Ye, Q. (2017). Optimal rebate strategies under dynamic pricing. Operations Research, 65(6), 1546-1561.

Zhao, H., Huang, H., & Li, X. (2025, November). PP-Pose: Privacy-Preserving Human Pose Estimation Using Random High-Frequency Channel Combinations. In Australasian Joint Conference on Artificial Intelligence (pp. 191-203). Singapore: Springer Nature Singapore.

Yang, Z., Liang, B., & Ji, W. (2021). An intelligent end–edge–cloud architecture for visual IoT-assisted healthcare systems. IEEE internet of things journal, 8(23), 16779-16786.

Wang, S., Zhang, X., Wang, P., & Li, X. (2026). Design of Magnetic Sensor Array-Based PUFs for IoT Security. IEEE Transactions on Instrumentation and Measurement, 75, 1-9.

Yang, Z., Ji, W., Guo, Q., Zhao, J., Zhao, C., Zhang, X., ... & You, Y. (2026). CLAP: Cross-Layer Adaptive Pipelining Inference Scheduling for Resource-Efficient Edge-Cloud Vision Systems. ACM Transactions on Architecture and Code Optimization.

Shen, B., Wang, Y., Shang, D., & Ning, T. (2026). Self-Commitment Latency: A Reward-Free Probe for Prompted Implicit Hacking. Publication date: 2026-06-04.

Jia, Y., Liu, X., Huang, J., Fan, Z., & Wang, X. (2026). Identity awakening in digital marketing: how facial recognition interactions foster green consumption behavior. Journal of Research in Interactive Marketing, 1-18.

Yang, Z., Ji, W., & Wang, Z. (2024). Adaptive joint configuration optimization for collaborative inference in edge-cloud systems. Science China Information Sciences, 67(4), 149103.

Luo, H., Li, Q., Cheng, H., Li, W., Sun, W., Zhao, W., & Liu, Z. (2025). A²Tformer: Addressing temporal bias and non-stationarity in transformer-based IoT time series classification. IEEE Internet of Things Journal, 12(20), 42198–42213.

Hu, Y., Yang, Z., Zhao, C., & Ji, W. (2026, May). Adaptive guidance semantically enhanced via multimodal llm for edge-cloud object detection. In ICASSP 2026-2026 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 12962-12966). IEEE.

Guo, J., Huang, S., Yao, Z., Zhang, Y., Lu, Y., Liu, J., ... & Wang, M. (2025). CryptoBench: A Dynamic Benchmark for Expert-Level Evaluation of LLM Agents in Cryptocurrency. arXiv preprint arXiv:2512.00417.

Cohen, J., Rosenfeld, E., & Kolter, J. Z. (2019). Certified adversarial robustness via randomized smoothing. In Proceedings of ICML.

Li, C., Chen, H., & Cai, W. (2026, April). From Slang to Standards: Consensus-Driven Airdrop Hunter Definition as a Baseline for Cryptocurrency Ecosystem Security and Governance. In Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (pp. 1-18).

Li, X., Wang, P., Li, G., Ni, L., & Zhang, Y. (2023). Design of interface circuits and lightweight PUF for TMR sensors. IEEE Sensors Journal, 23(11), 11754-11761.

Qu, D., & Ma, Y. (2025, August). Edge–Mesh–Ledger: Federated AI and Blockchain Framework for Scalable Global Sustainability Solutions. In 2025 International Conference on Artificial Intelligence for Sustainable Innovation (AI-SI) (pp. 1-6). IEEE.

Zhou, D. (2026). AI-Driven Hybrid SAST–DAST–SCA–IAST Framework for Risk-Based Vulnerability Prioritization in Microservice Architectures.

Zhao, Y., & Han, Z. (2025, December). Safe and Adaptive Cloud Healing: Verifying LLM-Generated Recovery Plans with a Neural-Symbolic World Model. In 2025 7th International Academic Exchange Conference on Science and Technology Innovation (IAECST) (pp. 89-94). IEEE.

Guo, Hanzhong, et al. "Real-time identity defenses against malicious personalization of diffusion models." arXiv preprint arXiv:2412.09844 (2024).

Li, S. (2025). Momentum, volume and investor sentiment study for us technology sector stocks—A hidden markov model based principal component analysis. PloS one, 20(9), e0331658.

Yang, Z., Ji, W., Guo, Q., & Wang, Z. (2023, October). Javp: Joint-aware video processing with edge-cloud collaboration for dnn inference. In Proceedings of the 31st ACM International Conference on Multimedia (pp. 9152-9160).

Wuyang Zhang and Shichao Pei. 2026. Your LLM Agent Can Leak Your Data: Data Exfiltration via Backdoored Tool Use. arXiv:2604.05432 [cs.CR] doi:10.48550/arXiv.2604.05432