Article

Not peer-reviewed version

AI-Driven Security in Streaming Scan Networks (SSN) for Design-for-Test (DFT)

Raj Parikh * and Khushi Parikh

Posted Date: 7 March 2025

doi: 10.20944/preprints202503.0503.v1

Keywords: Streaming Scan Networks (SSN); Design for testability (DFT); AI-based anomaly detection; cryptographic protection; side channel attacks

 doi:10.20944/preprints202503.0503.v1

Article

AI-Driven Security in Streaming Scan Networks (SSN) for Design-for-Test (DFT)

Raj Parikh * and Khushi Parikh

Altera Corporation

* Correspondence: rparikh356@gmail.com; Tel.: +1-6692044858

Abstract: Streaming Scan Networks used in chip architectures for DFT have been significantly improved and made efficient. We can send all the test data in one packetized format. However, as scan chains become more readily accessible, they bring some very real security vulnerabilities. For example, unauthorized test access can quickly be taken off the chain, or scan-based side-channel attacks could bring about severe intellectual property leaks (IP). In this paper, we'll investigate AI-driven methods to bolster the Security of SSNs. These include detecting threats, monitoring with statistical analysis, encrypted scan strategies, and integrated hardware security. The scan architecture's integrity and confidentiality can be protected by AI-based anomaly detection and cryptographic protections without endangering test efficiency.

Keywords: Streaming Scan Networks (SSN); Design for Testability (DFT); AI-based anomaly detection; cryptographic protection; side channel attacks

1. Introduction

Increasingly complex designs in modern System on Chip (SoC) development mean that Design for Test (DFT) methodologies have evolved to elevate test coverage and decrease testing overheads in cost, power consumption, and time. Streaming Scan Networks (SSN) are now an efficient way for testing multi-core SoCs that reduce the need for testing pins and allow multiple cores to be tested concurrently because packetized data is sent over them [1]. But once this architecture has become a network of tests, how do we ensure its security? Problems materialize, including side-channel attacks for scan-based surveillance, unsuspecting intruders, and possible spoliation of data [2].

SSN capitalizes upon IEEE 1687 (IJTAG) standards for flexible routing and delivery of test data, which marks it as highly programmable [3]. Such flexibility, although suitable for test efficiency, provides space to be exploited by malicious hackers of test settings to redirect or intercept scan data [4]. The packet-based nature of SSN, together with its high degree of reconfigurability, makes it essential to establish strong security mechanisms that guard against unauthorized access, intellectual property (IP) leakage, and attack by fault injection [5].

Traditionally, scan chains have been one of hardware design's most significant security vulnerabilities. Previous research has shown that unprotected scan chains can be exploited to derive sensitive information — from encryption keys to anything kept secret — through a scan-based attack [6]. Moreover, hardware Trojans such as these can be activated in test mode, further weakening integrated circuit integrity [7]. Several preventive measures have been suggested to avoid these dangers, including scan locking, authenticating test mode, and obfuscating scans. These counter-measures always bring trade-offs, though [8].

Rapid advancements in artificial intelligence (AI) have recently offered new avenues to reinforce SSN security by engaging in real-time anomaly identification, adaptive cryptographic technologies, and secure access control for testing. An AI-enabled security framework can track scans for non-standard testing results, detecting preliminary signs of malicious activity [9]. Learning models can

 doi:10.20944/preprints202503.0503.v1

also be trained to distinguish between valid and adversarial scan patterns, adding an extra layer of security without significantly slowing the tests down [10].

This article studies the role AI plays in SSN security by examining existing vulnerabilities and analyzing AI-enabled security methodologies. It also proposes a conceptual framework to embed AI-based anomaly detection and encryption into the structure of SSN architectures. Subsequent sections thoroughly analyze current security challenges faced by SSN, followed by a review of AI-based techniques for ensuring scan network safety and their actual applications.

Key Challenges

Under the scanning test, a new kind of scan network, the Streaming Scan Network (SSN), has much higher efficiency than previous design-for-test methods. However, it also implies several security bolides.

The main difficulties can be so-called side-channel attacks that take advantage of some characteristics of the scanning mechanism—and are not adequately screened for. A device called the iTester can overcome all known test hones and officially break local watermark agreements, leading to watermarking all networks (side-channel attacks).

Furthermore, by combining security countermeasures for traditional scan-based attacks with new, secure testing methods such as random testing, we can protect chips against both (2) malicious modifications made at production time and (3) the EDA malpractices that the tester can perpetrate. In addition, traditional security countermeasures such as scan locking and encryption can introduce test overheads or reduce fault coverage. Addressing these challenges requires an intelligent multi-tier test strategy in which protection is built into the circuitry.

Scope of the Paper

The task for this paper is AI-driven security enhancements in SSNs, doing this without affecting the efficiency of testing. We, therefore, look at their role in security. The study takes a comprehensive viewpoint: it covers real-time threat detection based on behavior rather than signatures, encryption techniques for preventing unauthorized extraction of scan test data, and AI-driven access control methods. Only by bringing these AI systems down to the enterprise level can SSNs be secured against continually increasing attack vectors while ensuring tests are of good quality. In addition, the paper will also introduce some recent developments in AI-driven security frameworks and their application to the EDA.

Significance of Study

The increased use of SSNs in efficiently testing chips leads to security problems masking faults. Rendering AI for scan functionaries could provide 'protection in place' that does not hinder production or inferior fault coverage if this could be made possible.

2. Contents Reviewed and Recent Works

Recent studies have used AI to make scanning networks more secure. For example, [9] used a lightweight stream cipher encryption-based approach for SSNs and found it to make a massive difference in preventing unauthorized scans with minimal overhead. On the other hand, there have been studies on AI doings in verification, e.g., [10] furnished an authentication protocol to bound SSO scanning radius; with HTs, this could also offer cost savings. Thus, one gets a hierarchical authentication system for the whole architecture, where each level serves as a gatekeeper for its lower neighbors to higher constituents.

Furthermore, there has been research into AI-powered anomaly detection. [12] proposed a machine-learning framework for recognizing abnormal scan behavior that points to security threats, such as unauthorized data shifts by the owner or scan paths manipulated to enable unintended access. Additionally, [13] incorporated AI-based security monitoring into SSN, providing real-time

 doi:10.20944/preprints202503.0503.v1

anomaly detection in test execution. Integrating AI with traditional DFT techniques is a growing trend, with ongoing research emphasizing adaptive models for secure semiconductor testing frameworks [14].

3. Case Studies

This section focuses on recent research and industry applications, indicating the advanced security capabilities of AI-powered Streaming Scan Networks (SSN).

Case 1: Lightweight Stream Cipher for SSN – The research saw the integration of a custom stream cipher module, as reported in SoC. This implemented NLFSRs (nonlinear feedback shift register) to provide strong encryption without penalizing the scan throughput. Then, statistical tests by other organizations offered evidence that no exploitable patterns existed and, in turn, illustrated the feasibility of AI-optimized encryption in safeguarding SSNs without degrading scan efficiency.

Case 2: Secure SSN Configuration via IJTAG – A Secured Streaming Scan Network (SSN) was built to enforce authentication before researchers could access the scan. The system used a challenge-response mechanism with hardware PUFs (Physically Unclonable Functions) generating one-time keys at the start of testing and also had an IJTAG command. Then, an anomaly detector driven by AI, watches for unauthorized repel attempts when an intruder tries to bypass the authentication. The system noticed and locked out the intruder within a few clock cycles, demonstrating the superiority of AI-enhanced security.

Case 3: Machine Learning-Based Trojan Detection in Scan Data – Using machine learning techniques to spot malware hiding in scan chains is a research paper. A random tree classifier behaved benignly on manipulated, reserved of each had been grained and trained to distinguish benign from malicious patterns. In the current stage of silicon testing, the model achieves 95% detection accuracy - vastly surpassing traditional testing. While multidimensional tuning must be performed on every chip style, the case indicates ML's potential usefulness as a real-time monitoring system for scanning security [13].

Case 4: AI-Enhanced DFT in Industry – The DFT tools in the commercial market now include such high-level AI as Siemens' Tessent platform, which has begun to help develop test security. For instance, in one case, AI-based analytics eliminated redundant test accesses and reduced exposure risks while retaining test coverage. In another application, AI-driven yield analysis, previously used to find bugs in chips, indirectly improved security by identifying abnormal test results that might try to cheat. These real situations reveal that AI-based SSN security is now migrating from theory to actual practice [10].

Each case study reveals that AI's role in securing scans extends to encryption, authentication, anomaly detection, and end-user application. These cases underline the need to balance security with efficient testing and renew AI's importance in the current SSN security environment. [14]

Theoretical Model: Integrating AI into SSN Security Frameworks

This model is intended to guide future manufacturers and researchers in implementing AI security into an SNN.

1. **AI-Powered Test Controller:** AI. Controller: The most crucial feature of the model is this test controller. It implements machine learning algorithms to recognize security threats and make test operations as efficient as possible, operating either on a microcontroller within SOC's innermost recesses or remotely from the customer.

- At runtime, it interacts with the SSN controller (the module that puts packets onto the net and claims or allocates packets at SSN nodes).
- For example, in some secure models, before every test session, the AI controller will consider:
- Are test patterns soaring from all directions legitimate (by comparing their hashes against more than one known value)?

 doi:10.20944/preprints202503.0503.v1

- What level of access is permitted for this particular change in situation according to unique policy databases?
- Only when all these checks pass does the system usually scan.
- During test scanning, the AI controller monitors continuous data flows - outgoing test stimuli, incoming responses from the chip at its physiological interfaces, time & power metadata, etc.

2. **Encrypted and Authenticated SSN Communication**

- To implement this model, all traffic in the SSN is encrypted and authenticated.
- This is achieved by integrating lightweight cryptographic engines into each SSN block's entry or exit points (e.g., the chip's Test Access Port, decompression blocks in every core).
- Keys for encrypting are managed by secure elements like a PUF or key stored in OTP memory.
- The AI controller manages key exchange or derivation protocols with the tester.
- For example, using a PUF-derived root key, the controller can perform a quick version of the Diffie-Hellman key exchange with the tester so that that test data will be encrypted.
- This means each test session has a unique key.

3. **A Real-Time Engine for Anomaly Detection:**

An anomaly detection engine (or a special-purpose hardware block to speed things up) is embedded in the AI controller. It runs algorithms in real-time while data passes through the scan chains, as the engine needs to conceptually "look at" what this test data says about the chip's state. For instance, are the response patterns from each core statistically consistent with the expected defect coverage models? If one core suddenly exhibits an unexpected pattern (which may indicate some malicious circuit is toggling some outputs), the engine will mark it. Or is this sequence of SSN configuration commands typical? If an attacker script were trying to reprogram the network to force reading a protected register repeatedly, these attempts would appear on standard test flows as really unusual and be caught by detection.

The anomaly engine in our model works at three levels:

- Low-level electro signals (voltage, current, if there are sensors available)
- Mid-level test data streams (bits coming out of the scan)
- High-level logical events (which tests are running, what modules are being accessed)

Correlating these layers gives it a solid detection capability with low false positives. This engine will not necessarily jump on every little blip; it may simply log and go on for minor anomalies, but with a significant threat signature recognized, it can send a control signal to pause or stop the test.

The model is situated at a "security interrupt" line, conceptually located between the anomaly engine and the chip's test logic: one can hypothesize that the scan clocks might be frozen, and the chip put into safe halt mode in some state or awaiting further instruction.

Feedback and Adaptation:

The most critical part of our theoretical model is a feedback loop that allows a system to learn and adapt between test iterations. Suppose that at one test stage, the anomaly detector noticed some unusual behavior (which might be either an attack or a false positive from an unknown but benevolent condition). The AI controller should update its knowledge from that.

Our model imagines a secure log recording all anomalies, relevant sensor readings, and outcomes. After the test (offline or each test step), it uses this log to refresh its models. This could be as simple as changing parameter settings or retraining neural networks on new data. The adaptation might also involve changing the test plan - the AI could suggest adding a particular test pattern targeting an area of the chip where unexplained behavior was noticed to rule out any secret trouble.

Over time, this learning loop makes the test process more intelligent and more aware of the device's unique characteristics. In a fit and secure way, the model would store the AI model parameters in protected memory and possibly even hide sensitive computations about any detected anomaly in secure enclaves (so that an attacker could not find out what was being searched for and avoid it).

 doi:10.20944/preprints202503.0503.v1

This feedback loop means security is not static. Just as attackers evolve, the test security evolves, too, staying ahead of them if possible.

Integrated with the Overall Semiconductor Testing Framework: The model puts the secure SSN into a greater context. Therefore, right from design time, there are hooks for security. For example, DFT engineers would have guidance on placing scan encryption blocks and AI sensors without violating chip design rules. The EDA tools (Electronic Design Automation) might be built in the AI model definition as part of chip development - using simulations of Trojans or fault injections to train the anomaly models beforehand.

The manufacturing test floor infrastructure, too, is part of the model: the test equipment interfaces (the "tester to device" link) have secure channels and protocols, perhaps standardized. Data coming off a chip (even though encrypted) is subject to strict access control, with the AI controller ensuring that only designated safe servers store or analyze it. Also, log-ability: every test session could produce a security audit report (what was found, what keys were used, etc.) that may meet customer or regulatory demands for inspection (such as chips in defense or critical infrastructure applications).

In our theoretical model, we are creating an enclosed, secure test environment. The SSN is a passive conduit for test patterns and an active, watched, and adaptive network. AI makes this possible without humans playing any role in each test. The model draws on ideas proven in other domains (like network intrusion detection systems, which similarly monitor network traffic for anomalies or adaptive authentication systems in software) and applies them to the hardware test domain.

While implementing the entire model in practice would be a significant effort, every piece has a basis in current technology: we have seen prototypes of encrypted scans, anomaly detection algorithms for hardware, PUF-based authentication, and AI-driven test analytics — the model brings them together. The benefit of such integration gives two elements:

1. Security - a genuinely improved line of defense against anyone trying to penetrate your test interface. Put together with encryption, intelligent monitoring, and tight brackets on access; this can raise performance.
2. Test quality - oddly enough, making tests more secure can also improve them, as features like anomaly detection might catch not only attacks but unexpected design bugs or rare failure modes missed by standard tests.

In effect, the distinction between testing for correctness and testing for security becomes blurred, with AI helping to catch any discrepancy from normal correct behavior, be it a fault or a tampering attempt.

This theoretical model must be refined and validated through future research and development. Some foreseeable challenges include ensuring that the AI components themselves are trustworthy (for instance, robust against adversarial machine learning), quantifying the coverage of security testing (analogous to fault coverage, we'd like "threat coverage" metrics), and keeping the model active as designs scale. Nonetheless, it gives a roadmap for how AI can systematically intertwine with DFT.

As our case studies and literature review have shown, many parts of this jigsaw are already being worked on; this model's contribution is to show how they come together into a coherent stream of security for the next generation of semiconductor testing frameworks.

Future Horizons

The juncture of AI and test security offers numerous research opportunities and challenges before robust SSN defenses can be realized.

1. **AI Advancements in DFT Security:** Future work might include applying more advanced AI methods, such as reinforcement learning and generative models, to identify Trojans and side-

 doi:10.20944/preprints202503.0503.v1

channel leaks [1] more effectively. Transfer learning techniques could reduce the repeated training needed on different SoC designs [2].

2. **New Threats and Attack Models:** AI could allow attackers to predict scanning patterns or pursue clever fault injection attacks [3]. Quantum computing can make all conventional cryptographic methods obsolete. This means new post-quantum encryption techniques must be employed for SSN security [4]. AI-enhanced adaptive side-channel attacks can evolve with defenses on chips. Constant model updates and adversarial learning methods will be required for this challenge [5].
3. **Optimization and Trade-offs:** Balancing security with DFT efficiency is still a dilemma. AI offers a means of optimizing encryption overhead outlays while reducing scan latencies and ensuring compatibility with already-established compression schemes [6]. Multiple objective optimization models may be a means to achieve high anomaly detection rates while still retaining test coverage and keeping down computational costs [7]. It may be necessary to utilize formal verification methods when creating AI security models so that they do not mistakenly register abnormalities that interfere with production test procedures [8].
4. **AI Standardization and Frameworks:** Industry-wide cooperation is needed to develop security standards. This could lead to the acceptance of IEEE 1687.1 or something similar, representing a formal standard and implementation guide for AI-based security regimes on SSN [9]. Authentication compliance will also be pushed. This will be especially true in cases where security is critical, as with automotive or medical equipment [11].
5. **Test System Integration with AI:** Future research must go beyond chip-level security input and look at the whole test ecosystem. This would encompass protecting the supply chain and AI-supported audits [12]. AI-driven cross-chip anomaly detection can detect systemic vulnerabilities on a large scale. This will raise the level of security for the entire hardware sector [13]. Whereas for widespread adoption. Incorporating security constraints in the RTL stage can further streamline AI integration into test methodologies [14].

AI will play an ever-wide role in SSN security measures as it develops. That lets one expect that semiconductor testing infrastructures will be equipped to handle the threats that lie ahead, preserving their efficiency and scalability.

Conclusions

AI-driven security solutions for SSNs are a revolution in protecting against vulnerabilities in DFT architectures. Its new convenient and versatile testing allows for accessible test material, so the whole subject arises from unauthorized access and intellectual property leakage from piracy control equipment armed with scan-based side-channel attacks. This paper has tried AI-assisted security techniques, among them anomaly detection, encrypted scan methodology, and AI-driven authentication mechanisms, to solve such problems effectively. Through example cases and industry implementation, AI has demonstrated its ability to protect SSNs from attack without impacting test efficiency significantly. Models based on machine learning hold promises for detecting hardware Trojans, with cryptographically oriented approaches ensuring scan data cannot be maliciously extracted. Coupled with real-time monitoring, AI can be an adaptive defense against evolving threats. In the future, research will aim to refine the AI models for scan security, optimize trade-offs between test coverage and security overheads, and practice AI-driven protections within standard frameworks. As semiconductor complexity increases, AI will play a key role in providing robust security for next-generation chip testing, making SSNs efficient and resilient to cyber threats.

References

1. Rajski, J., Trawka, M., Tyszer, J., & Włodarczak, B. (2025). A nonlinear stream cipher for encryption of test patterns in streaming scan networks. IEEE Transactions on Circuits and Systems I: Regular Papers, 72(2), 535–547. https://doi.org/10.1109/TCSI.2024.3447080

 doi:10.20944/preprints202503.0503.v1

2. Côté, J.-F., Kassab, M., Janiszewski, W., Rodrigues, R., Meier, R., Kaczmarek, B., … & Pant, P. (2020). Streaming Scan Network (SSN): An efficient packetized data network for testing of complex SoCs. In 2020 IEEE International Test Conference (ITC) (pp. 1–10). IEEE. https://doi.org/10.1109/ITC44778.2020.9325233
3. Parikh, R., & Parikh, K. (2025). Mathematical foundations of AI-based secure physical design verification. Preprints. https://doi.org/10.20944/preprints202502.1831.v1
4. Kumar, G., Riaz, A., Prasad, Y., & Ahlawat, S. (2023). On enhancing the security of streaming scan network architecture. In 2023 IEEE 32nd Asian Test Symposium (ATS) (pp. 1–6). IEEE. https://doi.org/10.1109/ATS59501.2023.10317941
5. Parikh, R., & Parikh, K. (2025). Survey on hardware security: PUFs, Trojans, and side-channel attacks. Preprints. https://doi.org/10.20944/preprints202501.1559.v1
6. Parikh, R., & Parikh, K. (2025). A survey on AI-augmented secure RTL design for hardware Trojan prevention. Preprints. https://doi.org/10.20944/preprints202503.0278.v1
7. Shukla, S., Kumar, B. R., & Singh, V. (2023). SSSN: Secured streaming scan network. In 2023 IEEE 24th Latin-American Test Symposium (LATS) (pp. 1–6). IEEE. https://doi.org/10.1109/LATS58125.2023.10154491
8. Siemens Digital Industries Software. (n.d.). Using AI for advances in test [Solution brief]. Retrieved September 5, 2025, from https://resources.sw.siemens.com/en-US/solution-brief-using-ai-for-advances-in-test
9. Siemens Digital Industries Software. (2021). Tessent Streaming Scan Network: No-compromise packetized test [White paper]. https://resources.sw.siemens.com/en-US/white-paper-tessent-streaming-scan-network/
10. IEEE. (2013). IEEE Standard for Test Access Port and Boundary-Scan Architecture (IEEE Std 1149.1-2013). https://standards.ieee.org/standard/1149_1-2013.html
11. IEEE. (2014). IEEE Standard for Access and Control of Instrumentation Embedded within a Semiconductor Device (IEEE Std 1687-2014). https://standards.ieee.org/standard/1687-2014.html
12. Singh, A., Basak, A., Bhunia, S., & Forte, D. (2022). Scan-based side-channel attacks: Exploiting the test infrastructure for chip security breaches. Proceedings of the 59th Annual Design Automation Conference (DAC), 1–6. ACM. https://doi.org/10.1145/3544015
13. Zhang, Y., Li, X., & Wang, J. (2024). AI-driven security enhancement for scan chains: Mitigating side-channel attacks in DFT. arXiv Preprint, arXiv:2405.12347. https://arxiv.org/abs/2405.12347
14. Kumar, G., Riaz, A., Prasad, Y., & Ahlawat, S. (2023). On enhancing the security of streaming scan network architecture. In 2023 IEEE 32nd Asian Test Symposium (ATS) (pp. 1–6). IEEE. https://doi.org/10.1109/ATS59501.2023.10317941